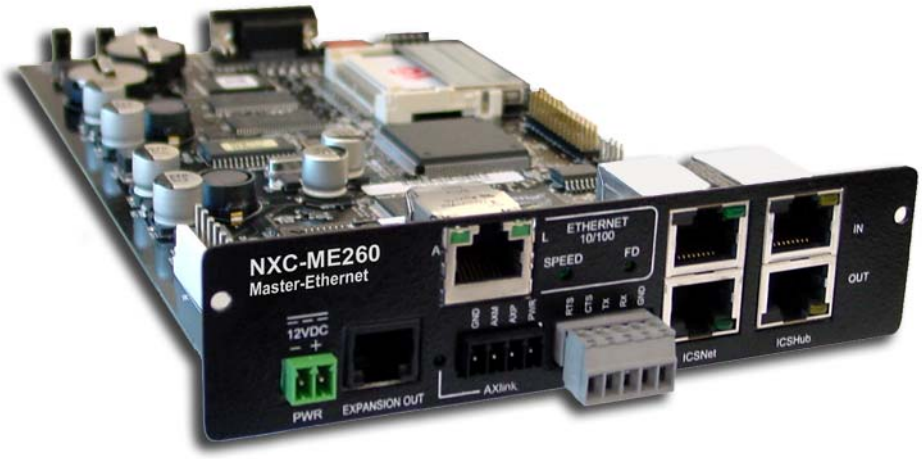
instruction manual

NXC-ME260

NetLinx Master-Ethernet Card/Module



NetLinx Central Controllers and Cards

AMX Limited Warranty and Disclaimer

AMX Corporation warrants its products to be free of defects in material and workmanship under normal use for three (3) years from the date of purchase from AMX Corporation, with the following exceptions:

- Electroluminescent and LCD Control Panels are warranted for three (3) years, except for the display and touch overlay components that are warranted for a period of one (1) year.
- Disk drive mechanisms, pan/tilt heads, power supplies, and MX Series products are warranted for a period of one (1) year.
- AMX Lighting products are guaranteed to switch on and off any load that is properly connected to our lighting products, as long as the AMX Lighting products are under warranty. AMX Corporation does guarantee the control of dimmable loads that are properly connected to our lighting products. The dimming performance or quality cannot be guaranteed due to the random combinations of dimmers, lamps and ballasts or transformers.
- Unless otherwise specified, OEM and custom products are warranted for a period of one (1) year.
- AMX Software is warranted for a period of ninety (90) days.
- Batteries and incandescent lamps are not covered under the warranty.

This warranty extends only to products purchased directly from AMX Corporation or an Authorized AMX Dealer.

All products returned to AMX require a Return Material Authorization (RMA) number. The RMA number is obtained from the AMX RMA Department. The RMA number must be clearly marked on the outside of each box. The RMA is valid for a 30-day period. After the 30-day period the RMA will be cancelled. Any shipments received not consistent with the RMA, or after the RMA is cancelled, will be refused. AMX is not responsible for products returned without a valid RMA number.

AMX Corporation is not liable for any damages caused by its products or for the failure of its products to perform. This includes any lost profits, lost savings, incidental damages, or consequential damages. AMX Corporation is not liable for any claim made by a third party or by an AMX Dealer for a third party.

This limitation of liability applies whether damages are sought, or a claim is made, under this warranty or as a tort claim (including negligence and strict product liability), a contract claim, or any other claim. This limitation of liability cannot be waived or amended by any person. This limitation of liability will be effective even if AMX Corporation or an authorized representative of AMX Corporation has been advised of the possibility of any such damages. This limitation of liability, however, will not apply to claims for personal injury.

Some states do not allow a limitation of how long an implied warranty last. Some states do not allow the limitation or exclusion of incidental or consequential damages for consumer products. In such states, the limitation or exclusion of the Limited Warranty may not apply. This Limited Warranty gives the owner specific legal rights. The owner may also have other rights that vary from state to state. The owner is advised to consult applicable state laws for full determination of rights.

EXCEPT AS EXPRESSLY SET FORTH IN THIS WARRANTY, AMX CORPORATION MAKES NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AMX CORPORATION EXPRESSLY DISCLAIMS ALL WARRANTIES NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED TO THE TERMS OF THIS LIMITED WARRANTY.

Table of Contents

Product Information

The NXC-ME260 (**FG2010-60**) is a Master-Ethernet Card for use within NetLinx systems. This card provides a 10/100 Base-T Ethernet connection and an RJ-11 SPE (Server Port Expander) connector for use with an AXB-SPE (Server Port Expander). The NXC-ME260 is the only Master card you will need, as it incorporates the functionality of all previous NetLinx Master Cards (NXC-M, NXC-ME, and NXC-MPE).

Beyond replacing the previous set of NetLinx Master Cards, the NXC-ME260 represents a high-performance NetLinx Master Controller. With double the Flash memory (16 MB) and a more powerful processor (Coldfire® 5407), the ME260 is faster than previous NetLinx Masters.

The NXC-ME260 can be loaded in the Master card slot of an NXF NetLinx Cardframe, in an NXI Integrated Controller, or within an NXS-MHS Master/Hub Module.

Front and rear panel components

FIG. 1 shows the front and rear panel components of the NXC-ME260.

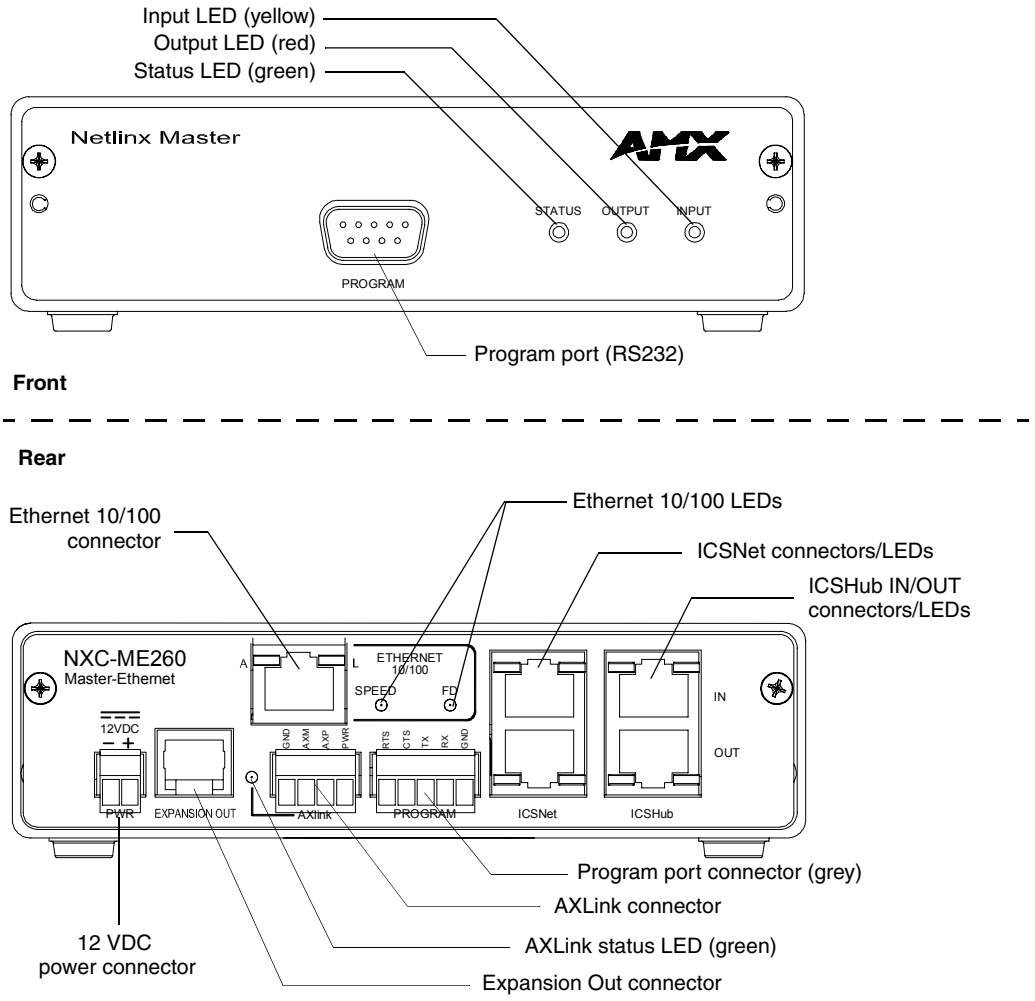


FIG. 1 Front and rear panel components (NXC-ME260 card shown installed within an NXS-MHS)

Specifications

NXC-ME260 Specifications	
Dimensions (HWD):	
NXC Card	1.38" x 5.43" x 9.25" (35.1 mm x 138.0 mm x 235.0 mm)
NXS Module	1.64" x 5.55" x 9.28" (41.7 mm x 141.0 mm x 236.0 mm)
Weight:	NXC-ME260 only: 0.55 lbs (0.25 kg) NXC-ME260 with NXS-NMS module: 1.95 lbs (0.88 kg)
Power Consumption:	750 mA @ 12 VDC
Memory:	Compact Flash: 32 MB standard (upgradeable) Volatile: 16 MB Non-volatile: 1 MB
Microprocessor:	Coldfire® 5407 (32-bit)
Enclosure:	Metal with black matte finish.
Front Faceplate:	Plastic grey with translucent viewing window.
Front Panel Components:	
Program port	DB9 (male) connector supports RS-232 communications to your PC for system programming and diagnostics. You set the port's communication speed with the Baud Rate DIP switch. See the *Setting the Program Port DIP Switch* section on page 5 for details. ***Note:*** There are Program ports located on the front and rear panels of the Master card for easy access. Because these ports share the same circuitry, you should never use both at the same time; doing so will result in communication and/or programming errors.
Status LED	Green LED lights to indicate that the system is programmed and communicating properly.
Output LED	Red LED lights when the Master transmits data, sets channels On and Off, sends data strings, etc.
Input LED	Yellow LED lights when the Master receives data from button pushes, strings, commands, channel levels, etc.
Front Panel LEDs - blink patterns	These LEDs also display special blink patterns when a mode is activated. See the *Modes and Front Panel LED Blink Patterns* section on page 7 for details.
Program Port DIP Switch	8-position DIP switch located behind the front panel for setting the baud rate for the Program port. • Available baud rate settings are 9600, 38,400 (default), 57,600 and 115,200 (bps). Refer to the *Setting the Program Port DIP Switch* section on page 5 for details.
Rear Panel Components:	
PWR connector	2-pin (male) green captive-wire connector for 12 VDC power supply.
EXPANSION OUT port	RJ11 connector connects to an AXB-SPE Server Port Expander.
Ethernet 10/100 port	RJ-45 Ethernet 10/100 connector. The Ethernet port automatically negotiates the connection speed (10 Mbps or 100 Mbps) and whether to use half duplex or full duplex mode.
Ethernet 10/100 LEDs	LEDs that show communication activity, connections, speeds, and mode information: • A-activity - Yellow LED blinks when receiving Ethernet data packets. • L-link - Green LED lights when the Ethernet cables are connected and terminated correctly. • SPEED - Green LED lights when transmitting data at 100 Mbps, and is Off when transmitting at 10 Mbps. • FD-full duplex - Green LED lights when running in full duplex mode, and is Off when running half duplex mode.

NXC-ME260 Specifications (Cont.)	
Rear Panel Components (Cont:)	
AXlink connector	4-pin (male) black captive-wire connector provides data and power to external control devices. • Power rating = 6 A max; actual load depends on connected power supply.
Axlink Status LED	Green LED lights to show AXlink and expansion port data activity.
Program port	5-pin (male) grey connector for system programming and diagnostics. There is a Program port located on the front and rear of the Master Cards for easy access. Because these ports share the same circuitry, you should never use both ports at the same time. Doing so will result in communication and/or programming errors.
ICSNet connectors	Two RJ-45 connectors that provide power (500 mA) and data to external ICSNet devices.
ICSNet LEDs	Green LEDs that light when receiving data on that port.
ICSHub In/Out connectors	Two RJ-45 connectors that provide data to other Hubs connected to the Master.
ICSHub IN/OUT LEDs	Yellow LEDs that light when receiving data on that port.
Included Accessories:	• Connector Bag containing: - One Green 2-pin 3.5 mm mini-Phoenix connector (female) (41-5025) - One Black 4-pin 3.5 mm mini-Phoenix connector (female) (41-5047) - One Grey 5-pin 3.5 mm mini-Phoenix connector (female) (41-5053) - One back panel (51-2010-61)
Optional Accessories:	• AC-RK Accessory Rack Kit (**FG515**) • PSN2.8: Power Supply (**FG423-17**) with 3.5 mm mini-Phoenix connector • PSN4.4: Power Supply (**FG423-45**) with 3.5 mm mini-Phoenix connector • PSN6.5: Power Supply (**FG423-41**) with 3.5 mm mini-Phoenix connector

Rear panel LEDs: ICSNet/ICSHub

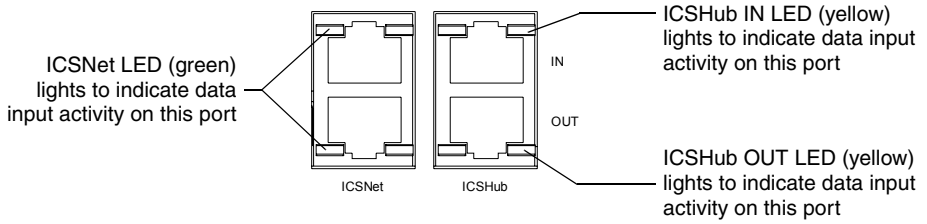


FIG. 2 Layouts of the ICSNet and ICSHub LEDs

Rear panel LEDs: Ethernet

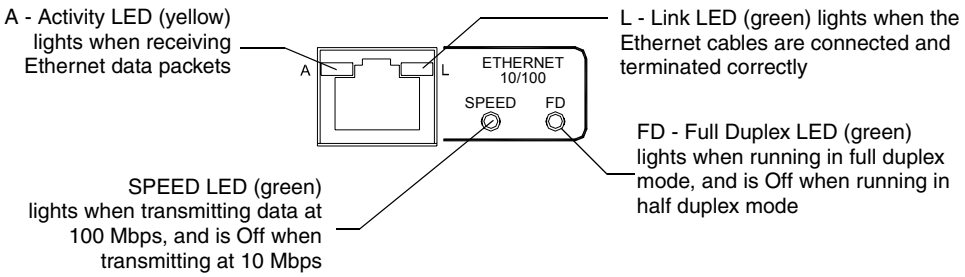


FIG. 3 Layout of Ethernet LEDs

Installation and Wiring

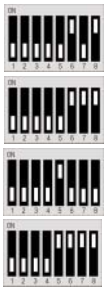
This section contains information about configuring the Program port, cable configurations, connector pinouts, and NXC-ME260 installation procedures.

Setting the Program Port DIP Switch

Prior to installing the NXC-ME260, configure the Program port's communication speed by setting the baud rate DIP switch (SW1) to the appropriate setting. The Program port's DIP switch is located to one side of the Master's RS232 Program port.

Baud rate settings

The Program port DIP switch is located on the Master card's circuit board. Use this DIP switch to set the baud rate used by the Program port for communication. Before programming the Master, make sure the baud rate you set matches the communication set on either your PC's COM port or through your NetLinx Studio 2.1. By default, the baud rate is set to 38,400 (bps).

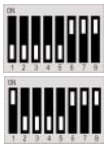


Baud Rate Settings				
Baud Rate	**Position 5**	**Position 6**	**Position 7**	**Position 8**
9600 bps	OFF	ON	OFF	ON
38,400 bps (default)	OFF	ON	ON	ON
57,600 bps	ON	OFF	OFF	OFF
115,200 bps	ON	ON	ON	ON

Note the orientation of the DIP Switch and the ON position label.
DIP Switch positions 2,3, and 4 must remain in the OFF position at all times.

Program Run Disable (PRD) mode

You can also use the Program Port DIP switch to set the Master card to Program Run Disable (PRD) mode according to the settings listed in the table below.



PRD Mode Settings	
PRD Mode	**Position 1**
Normal mode (default)	OFF
PRD Mode	ON

PRD mode prevents the NetLinx program stored in the Master from running when you power up the NXC-ME260. PRD mode should only be used when you suspect the resident NetLinx program is causing inadvertent communication and/or control problems. If necessary, place the Master in PRD mode and use the NetLinx Studio 2.1 program to resolve the communication and/or control problems with the resident NetLinx program. Then, download the new NetLinx program and try again.

NOTE

Think of the PRD Mode (On) equating to a PC's SAFE Mode setting. This mode allows a user to continue powering a unit, update the firmware, and download a new program while circumventing any problems with a currently downloaded program. Power must be cycled to the unit after activating/deactivating this mode on the rear Program Port DIP switch #1.

Setting the Program Port DIP switch

It is recommended that the baud rate DIP switch be set prior to any installation of the NXC-ME260 card.

1. Locate the red baud rate DIP switch (FIG. 4).
2. Set DIP switch positions according to the information listed in the *Baud Rate Settings* and *PRD Mode Settings* tables above.
3. Follow the procedures outlined in the *NXC-ME260 Installation and Mounting Procedures* section on page 15.

If the card has already been installed:

1. Disconnect the power supply from the 2-pin PWR (green) connector on the Master Card.
2. Unsecure the NXC-ME260 by unscrewing the two faceplate securing screws (on both sides of the faceplate) using a Phillips-head screwdriver (FIG. 4).
3. Carefully slide-out the card and locate the red baud rate DIP switch (FIG. 4).
4. Set the DIP switch positions according to the information listed in the *Baud Rate Settings* and *PRD Mode Settings* tables (page 5).
5. Place the Master card back into its' housing and resecure the two faceplate securing screws.
6. Reconnect the 12 VDC power supply to the 2-pin PWR connector and apply power.

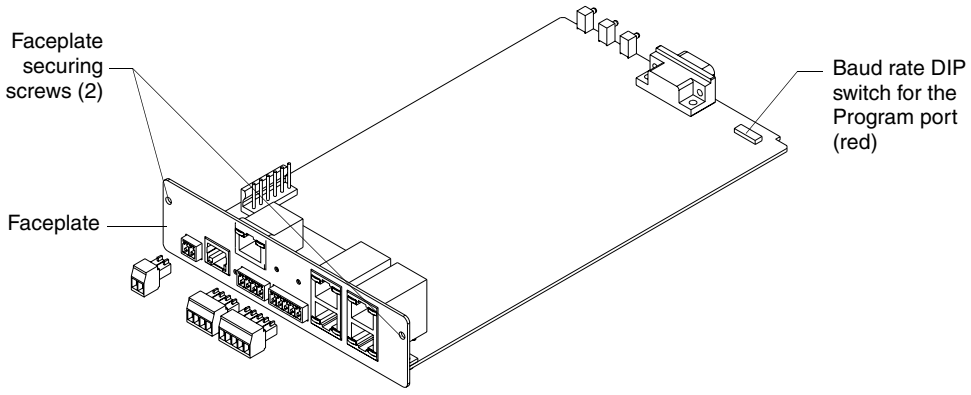


FIG. 4 Component locations on the NXC-ME260

Modes and Front Panel LED Blink Patterns

The following table lists the modes for the ME260 and blink patterns displayed on the front panel LEDs for each mode. *These patterns are not evident until after the unit is powered.*

Modes and LED Blink Patterns

Mode	Description	LEDs and Blink Patterns		
		STATUS (green)	OUTPUT (red)	INPUT (yellow)
OS Start	Starting the operating system (OS).	On	On	On
Boot	Master is booting.	On	Off	On
Contacting DHCP server	Master is contacting a DHCP server for IP configuration information.	On	Off	Fast Blink
Unknown DHCP server	Master could not find the DHCP server.	Fast Blink	Off	Off
Downloading Boot firmware	Downloading Boot firmware to the Master Card's on-board flash memory. *Do not cycle power during this process!*	Fast Blink	Fast Blink	Fast Blink
No program running	There is no program loaded, or the program is disabled.	On	Normal	Normal
Normal	Master is functioning normally.	1 blink per second	Indicates activity	Indicates activity

Wiring Guidelines

The Master card requires 12 VDC power from either a PSN2.8, PSN4.4, or a PSN6.5 NetLinx Power Supply to operate properly. The NXC-ME260 connects to the power supply via a 2-pin 3.5 mm mini-Phoenix connector located on the faceplate.

WARNING

This unit should only have one source of incoming power. Using more than one source of power to the Master card can result in damage to the internal components and a possible burn out.
Apply power to the card only after installation is complete.

Preparing captive wires

You will need a wire stripper and flat-blade screwdriver to prepare and connect the captive wires.

WARNING

Never pre-tin wires for compression-type connections.

1. Strip 0.25 inch (6.35 mm) of insulation off all wires.
2. Insert each wire into the appropriate opening on the connector (according to the wiring diagrams and connector types described in this section).
3. Tighten the screws to secure the wire in the connector. Do not tighten the screws excessively; doing so may strip the threads and damage the connector.

Wiring length guidelines

The Master requires a 12 VDC power from a PSN to operate properly. The unit should only have one source of incoming power.

WARNING

Using more than one source of power to the Master can result in damage to the internal components and a possible burn out.

An auxiliary 12 VDC power supply can provide power to the Master. Refer to the following table for wiring length information:

Wiring Length Guidelines @ 750 mA	
Wire Size	**Maximum wiring length**
18 AWG	156.49 feet (46.69 meters)
20 AWG	99.01 feet (30.18 meters)
22 AWG	61.73 feet (18.81 meters)
24 AWG	38.91 feet (11.86 meters)

Wiring a 2-pin power connection

To use the NetLinx 2-pin 3.5 mm mini-Phoenix power supply jack for power transfer from the PSN power supply to the rear of the NXC-ME260, the incoming PWR and GND cables from the PSN must be connected to its corresponding location on the 2-pin 3.5 mm mini-Phoenix connector (FIG. 5).

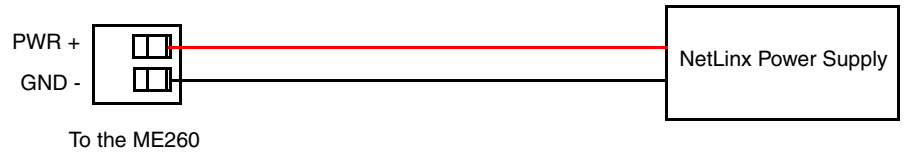


FIG. 5 2-pin mini-Phoenix connector wiring diagram (direct power)

Using the 4-pin mini-Phoenix connector for data and power

Connect the 4-pin 3.5 mm mini-Phoenix (female) captive-wire connector to an external Netlinx device, as shown in FIG. 6.

FIG. 6 4-pin mini-Phoenix connector wiring diagram (direct data and power)

Using the 4-pin mini-Phoenix connector for data with external power

To use the NetLinx 4-pin 3.5 mm mini-Phoenix (female) captive-wire connector for data communication and power transfer; the incoming PWR and GND cable from the PSN must be connected to the AXlink cable connector going to the NXC-ME260. FIG. 7 shows the wiring diagram. Always use a local power supply to power the Master card.

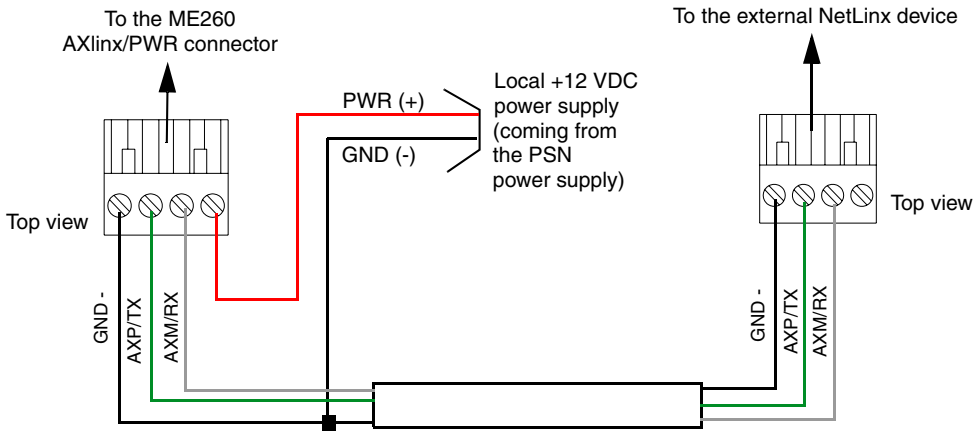


FIG. 7 4-pin mini-Phoenix connector wiring diagram (using external power source)

WARNING

*When connecting an external power supply, do not connect the wire from the PWR terminal (coming from the external device) to the PWR terminal on the Phoenix connector attached to the NXC-ME260. Make sure to connect **only** the AXM, AXP, and GND wires to the Master's Phoenix connector when using an external PSN power supply.*

Make sure to connect only the GND wire on the AXlink/PWR connector when using a separate 12 VDC power supply. Do not connect the PWR wire to the AXlink connector's PWR (+) opening.

Program Port Connections and Wiring

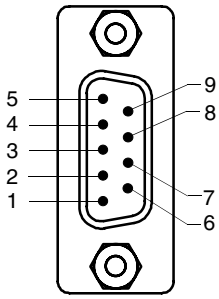
The NXC-ME260 is equipped with two Program ports. One is located on the front panel and the other is on the rear for easy access. The port on the front panel is an RS232 (male) connector and the rear port is a grey 5-pin (male) connector.

Use a Programming cable to connect the Program port to your PC's COM port to communicate with the Master card. Then, you can download NetLinx programs to the Master card using the NetLinx Studio 2.1 software program. Refer to the *NetLinx Studio* instruction manual for programming instructions.

RS232 Program port (front panel)

The following table shows the front panel RS232 (DB9) Program Port connector (male), pinouts, and signals.

RS232 Program Port, Pinouts, and Signals

Program Port Connector	Pin	Signal
 Male	2	RX
	3	TX
	5	GND
	7	RTS
	8	CTS

5-Pin Program port (rear panel)

The table below lists the pinouts and signals for the grey rear panel 5-pin 3.5 mm mini-Phoenix Program port connector.

5-Pin Program Port Pinouts and Signals

Pin	Signal
1	GND
2	RX
3	TX
4	CTS
5	RTS

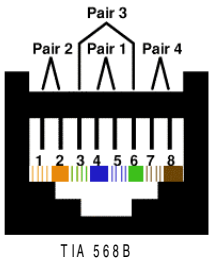
ICSNet RJ-45 Connections/Wiring

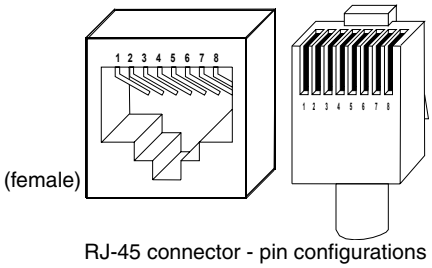
The following table shows the pinouts, signals, and pairing information to use for ICSNet RJ-45 connections. The ICSNet connections provide power and data to ICSNet devices. Each port provides up to 500 mA of current.

ICSNet RJ-45 Signals

Pin	Signal-Master	Signal-Device
1	TX +	RX +
2	TX -	RX -
3	N/A	N/A
4	GND	GND
5	N/A	N/A
6	N/A	N/A
7	RX +	TX +
8	RX -	TX -

RJ-45 Pinout Information (EIA/TIA 568 B)			
Pin	**Wire Color**	**Polarity**	**Function**
1	Orange/White	+	Transmit
2	Orange	-	Transmit
3	Green/White	-	Mic
4	Blue	-	Ground
5	White/Blue	+	12 VDC
6	Green	+	Mic
7	White/Brown	+	Receive
8	Brown	-	Receive





RJ-45 connector - pin configurations

NOTE

Unlike the ICSNet ports, the ICSHub connections require a specific polarity. The IN/OUT configuration, on the Hub ports, was implemented to use the same cables as ICSNet, but these ports need TX and RX crossed. You must connect an OUT to an IN, or an IN to an OUT port.
This is done simply to keep the polarity straight. The Hub bus is still a bus. All Hub connections are bi-directional.

ICSHub RJ-45 Connections/Wiring

The two ICSHub RJ-45 connectors on the rear of the Master card provide data to other Hubs connected to a downstream system. Hubs allow you to connect multiple NetLinx Hubs together in a daisy-chain configuration. Connect the OUT port to the IN port on the second or downstream NetLinx Hub.

- Use CAT5 cables for all ICSHub connections.
- **Do not** connect the last hub in a daisy-chain configuration into the first Hub.

ICSHub IN port

The following table describes the pinout and signal information for the ICSHub IN port.

ICSHub IN Pinouts and Signals		
Pin	**Signal**	**Color**
1	TX -	orange-white
2	TX +	orange
3	------	------
4	------	------
5	------	------
6	------	------
7	RX -	brown-white
8	RX +	brown

ICSHub OUT port

The following table describes the pinout and signal information for the ICSHub OUT port.

ICSHub OUT Pinouts and Signals		
Pin	**Signal**	**Color**
1	RX +	orange-white
2	RX -	orange
3	------	------
4	------	------
5	------	------
6	------	------
7	TX +	brown-white
8	TX -	brown

Ethernet 10/100 Base-T RJ-45 Connections/Wiring

The following table lists the pinouts and signals associated to the Ethernet connector. FIG. 8 describes the RJ-45 pinouts, signals, and pairing for the Ethernet 10/100 Base-T RJ-45 connector and cable.

Ethernet RJ-45 Pinouts and Signals				
Pin	**Signals**	**Connections**	**Pairing**	**Color**
1	TX +	1 --------- 1	1 --------- 2	orange-white
2	TX -	2 --------- 2		orange
3	RX +	3 --------- 3	3 --------- 6	green-white
4	no connection	4 --------- 4		blue
5	no connection	5 --------- 5	4 --------- 5	blue-white
6	RX -	6 --------- 6		green
7	no connection	7 --------- 7	7 --------- 8	brown-white
8	no connection	8 --------- 8		brown

FIG. 8 diagrams the RJ-45 cable and connectors.

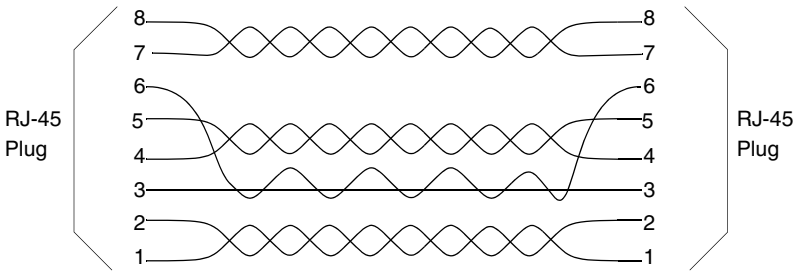


FIG. 8 RJ-45 wiring diagram

Ethernet ports used by the ME260

Ethernet Ports Used by the ME260		
Port type	**Description**	**Standard Port #**
ICSP	Peer-to-peer protocol used for both Master-to-Master and Master-to-device communications. For maximum flexibility, the Master can be configured to utilize a different port than 1319, or disable ICSP over Ethernet completely from either Telnet or the Program Port located on the rear of the Master itself.	1319 (UDP/TCP)
ICMP	When using version 1.XX of NetLinx Studio, you must be able to PING a Master in order to be able to connect to it over a network. • ***Note:*** *NetLinx Studio version 2.0 or higher allows a user the ability to turn Off this requirement by de-selecting the "Automatically Ping the Master Controller to ensure availability" feature from within the TCP/IP Setting dialog (default condition is On).*	ICMP
Telnet	The NetLinx telnet server provides a mechanism to configure and diagnose a NetLinx system. For maximum flexibility, the Master can be configured to utilize a different port than 23, or disable Telnet completely from either Telnet or the Program Port located on the rear of the Master itself. Once disabled, the only way to enable Telnet again is from the Master's Program port.	23 (TCP)
HTTP	The Master has a built-in web server that complies with the HTTP 1.0 specification and supports all of the required features of HTTP v1.1.	80 (TCP)
FTP	The NXC-ME260 has a built-in FTP server that conforms to RFC959.	21/20 (TCP)
Internet Inside	The Internet Inside feature the Master uses, by default, is port 10500 for the XML based communication protocol. This port is connected to by the client web browser's JVM when Internet Inside control pages are retrieved from the on-board Master's web server. For maximum flexibility, the on-board Master can be configured to utilize a different port than 10500 or to disable Internet Inside completely.	10500 (TCP)

SPE Port Connection/Wiring

Use an RJ-11 cable to connect the NXC-ME260 to an AXB-SPE Slave Port Expander.

The EXPANSION OUT port on the rear panel of the NXC-ME260 connects to the EXPANSION IN port on the rear panel of the AXB-SPE (FIG. 9).

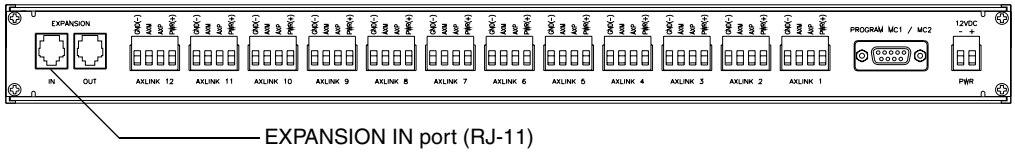


FIG. 9 AXB-SPE (rear panel)

You can daisy chain multiple AXB-SPE's by connecting the EXPANSION OUT on the primary AXB-SPE to the EXPANSION IN port on the secondary, as shown in FIG. 10. The connecting RJ-11 cable should not exceed 6" in length. Repeat this process to connect up to nine AXB-SPE's.

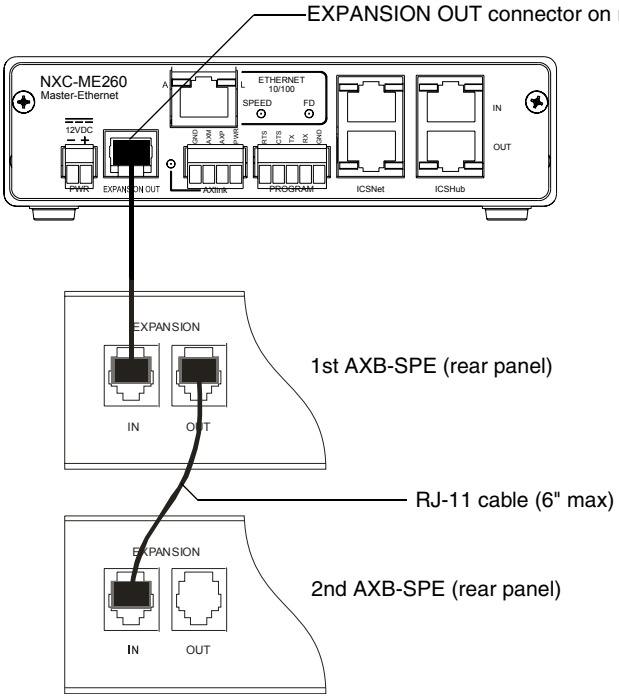


FIG. 10 Daisy chaining two or more AXB-SPE's off of an NXC-ME260

SPE cable pinout information

The following table gives pinout information for the RJ-11 SPE connector. AMX supplies a 6" RJ-11 cable with the AXB-SPE. The EXPANSION connectors (on the AXB-SPE) use pins 2, 3, 4 and 5. *Pin 2 is Ground; the others are all pin-to-pin connections.*

SPE Connector Pinouts and Signals	
Pin	**Signal**
1	no connect
2	GND
3	TX
4	TX enable
5	RX
6	no connect

NOTE

Do not use a standard phone extension cable; it will not work with the AXB-SPE.

FIG. 11 diagrams the RJ-11 cable and connectors.

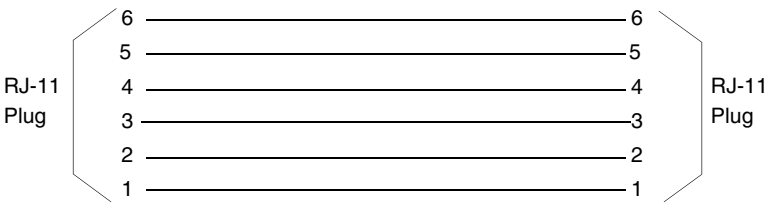


FIG. 11 RJ-11 wiring diagram

NXC-ME260 Installation and Mounting Procedures

Mounting the ME260 into an NXS-NMS

1. Confirm the contents of the shipment box to verify that you have all specified parts. Refer to the *NXC-ME260 Specifications* section on page 2 for more information about included and optional accessories.
2. Carefully remove the NXS-NMS Master/Hub Module from the shipping box.
3. Pull-away the magnetic faceplate from the front of the NXS-NMS. This exposes the front panel LEDs and Program port opening (FIG. 12).
4. Carefully remove the NXC-ME260 from its anti-static bag and place it aside.
5. Grasp the NXC-ME260 by the faceplate and direct the Program port (on the front of the card) into the opening on the rear of the NXS-NMS (FIG. 12).
6. Slide the Master card along the lowest pair of internal guide slots within the NXS-NMS.

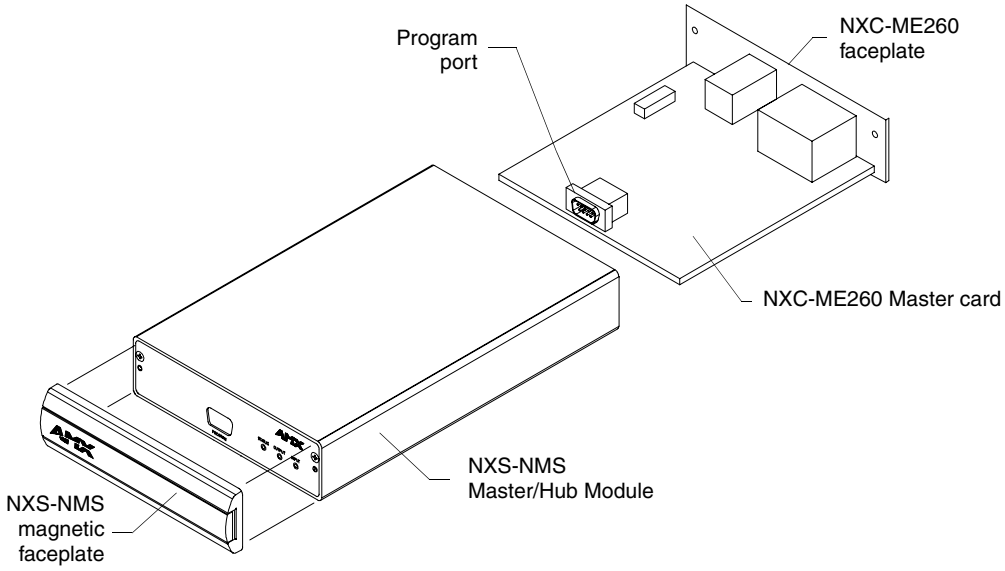


FIG. 12 Component locations on both NXC-ME260 and NXS-NMS

7. Secure the NXC-ME260 faceplate to the NXS-NMS by using a Phillips-head screwdriver to turn the two faceplate securing screws in a clockwise direction.
8. Connect the 12 VDC power supply to the 2-pin PWR connector and apply power.

Mounting the NXS-NMS Into an Equipment Rack

To install the Master/Hub Module into an optional AC-RK equipment rack:

1. Remove the front panel from the Module to expose the mounting holes.
2. Mount the module on the AC-RK bracket.
3. Place the AC-RK bracket (with the module) in the equipment rack and secure the bracket to the rack.
4. Replace the front panel to the Module, and reattach the plastic faceplate (if necessary).

Mounting the NXC-ME260 in an NXF CardFrame or NXI

The NXC-ME260 can be installed in a NetLinx CardFrame (NXF) or NetLinx Integrated Controller (NXI). In both cases, the card mounts in a horizontal position, through the Master card slot on the rear panel of the enclosure.

FIG. 13 shows the Master Card slot on the NXF CardFrame.

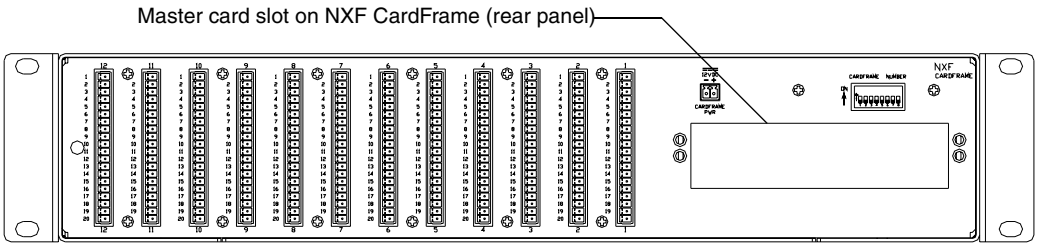


FIG. 13 Master card slot on rear panel of the NXF CardFrame

FIG. 14 shows the Master card slot on the NXI Integrated Controller.

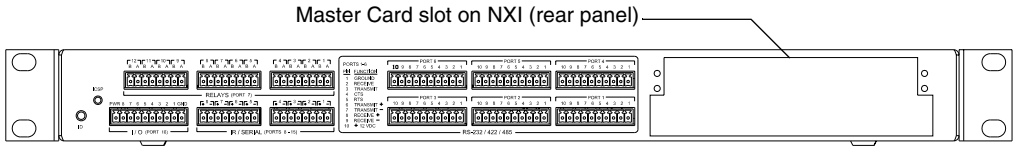


FIG. 14 Master card slot on rear panel of the NXI Integrated Controller

To install a Master card into either an NXF CardFrame or NXI Integrated Controller:

1. Discharge the static electricity from your body by touching a grounded object.
2. Unplug all the connectors from the Controller or Module.
3. Unscrew the two screws that hold the front faceplate plate on the Master card and remove the front plate.
4. Align the edges of the card with the guide slots inside the Master card slot on the NXF or NXI.
5. Slide the card about halfway into the slot.
6. Inside the Master card slot on the NXF or NXI, find the 6-pin control cable connector.
7. Plug the connector from the NXF or NXI into the 6-pin terminal on the Master card. This connector is keyed to ensure correct orientation.
8. Once the control cable is connected, gently slide the card all the way in until you feel the rear edge of the card lightly snap into place.
9. Re-apply power and other connections as necessary.

Replacing the Lithium Batteries

The NXC-ME260 is equipped with two lithium batteries (**FG57-0013**) that have a life of approximately 2.5 years to protect their memory. When DC power is on, the batteries (FIG. 15) are not used. When replacing the batteries, remove one at a time to avoid losing the program in memory.

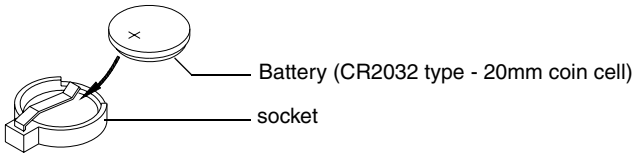


FIG. 15 Lithium battery and socket

1. Discharge the static electricity from your body by touching a grounded metal object.
2. Unplug all the connectors from the Controller or Module.
   - NetLinx Integrated Controller (NXI): Remove the rear panel from the NXI. Then, disconnect the NXI control cable and remove the Master card.
   - NetLinx Module (NXS-xxx): Remove the rear panel from the Module, and remove the Master card.
3. Locate the two batteries behind the Program port on the NXC-ME260 circuit board.
4. Carefully slide one battery out of its socket and insert the new battery.
5. Plug the 2-pin PWR (green) connector to reapply power. Wait approximately 1 minute. Then, remove the PWR connector again.
6. Carefully slide the other battery out of its socket and insert the new battery.
7. Replace the Master card (re-connect the NXI control cable to the Master card if replacing in an NXI).
8. Replace and resecure the rear faceplate using the mounting screws and reconnect all communication connectors.
9. Reconnect the 12 VDC power supply to the respective PWR connector and apply power.

Communication and Firmware Update

This section outlines the steps necessary to setup a NetLinx Master for communication and then update the on-board firmware.

WARNING

*Verify that the NetLinx Master firmware is **build 139.** Later versions of firmware can not be used on this ME260 Master.*

Before beginning:

1. Setup and configure your NXC-ME260. Refer to the *Installation and Wiring* section on page 5 for setup procedures.
2. Verify that you have the latest NetLinx Studio installed on your PC.
3. If necessary, download the latest Studio software from **www.amx.com > Tech Center > Downloadable Files > Application Files > NetLinx Studio 2.1**. This program is used to setup a System number, obtain/assign the IP/URL for the connected NetLinx Master, and transfer firmware KIT files to the Master.
4. Verify that an Ethernet/ICSNet cable is connected from the rear of the unit to its' respective connector on the Ethernet Hub (***for IP/ICSNet communication***).
5. Connect an RS-232 programming cable from the front of the NetLinx Master to the rear connector (COM port) on the PC being used for programming (***for DB9 communication***).
6. Verify that the NetLinx Master is receiving power and is turned On.

NOTE

If you have previously setup communication with your Master via an IP Address, continue with the firmware update procedures outlined in the Communicating with the NetLinx Master via an IP section on page 28.

Communicating with the Master via the Program Port

1. Launch NetLinx Studio 2.1 (default location is **Start >Programs > AMX Control Disc > NetLinx Studio > NetLinx Studio 2.1**).
2. Select **Settings > Master Communication Settings**, from the Main menu, to open the Master Communication Settings dialog (FIG. 16).
3. Click the **Communications Settings** button to open the Communications Settings dialog (FIG. 16).
4. Click the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working with a NetLinx Master (such as the NXC-ME260 or NI-Series of Integrated Controllers).
5. Click the **Serial** radio button (*from the Transport Connection Option section*) to indicate you are connecting to the Master via a (Serial) COM port.
6. Click the **Edit Settings** button to open the Serial Settings dialog (FIG. 16).

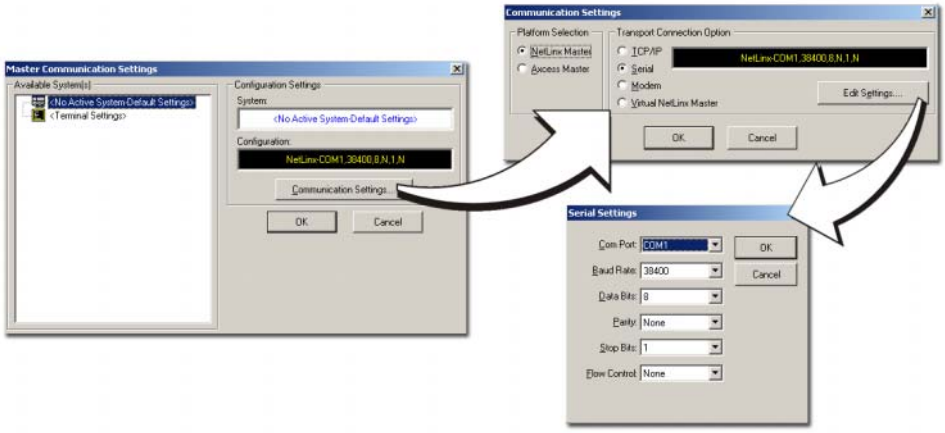


FIG. 16 Assigning Communication Settings and Baud Rates

7. Set the COM port parameters for the selected COM port being used for communication to the NetLinx Master. ***Default parameters are: COM1, 38400, 8 Data Bits, No Parity, 1 Stop Bit, and No Flow Control.***
8. Click **OK** three times to close the open dialogs and save your settings.

NOTE

If the connection fails to establish:
*Select a different COM port, press the **Retry** button to reconnect using the same communication parameters, or press the **Change** button to alter your communication parameters and repeat steps 2 thru 8.*

Verifying the current version of NetLinx Master firmware

1. Click on the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
2. Right-click on the *Empty Device Tree* entry and select **Refresh System** to establish a new connection to the System's Master and refresh the list with online system devices. *The communication method is highlighted in green on the bottom of the NetLinx Studio window.*

NOTE

The current firmware version of the Master is displayed to the right of the device.

3. After the Communication Verification dialog window verifies active communication between the PC and the Master, verify the NetLinx Master appears in the **OnLine Tree** tab of the Workspace window (FIG. 17).
4. If the firmware version is not **build 139** (v2_XX_**139**) for the NXC-ME260, follow the procedures outlined in the following sections to assign System/Device values, setup an IP Address, and then transfer the new firmware KIT file to the Master.

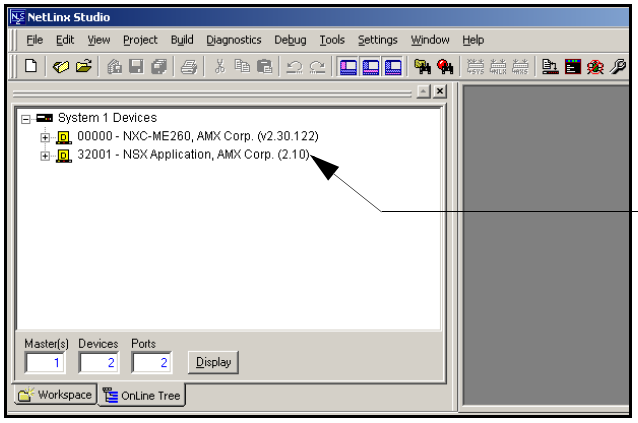


FIG. 17 Initial NetLinx Workspace window (showing the OnLine Tree tab)

Setting the System Value

1. Access/open the Device Addressing dialog (FIG. 18) by either one of these two methods:
   - Right-click on any System item listed in the **OnLine Tree** tab of the Workspace and select **Device Addressing** (from the pop-up list).
   - Select **Diagnostics** > **Device Addressing** from the Main menu.

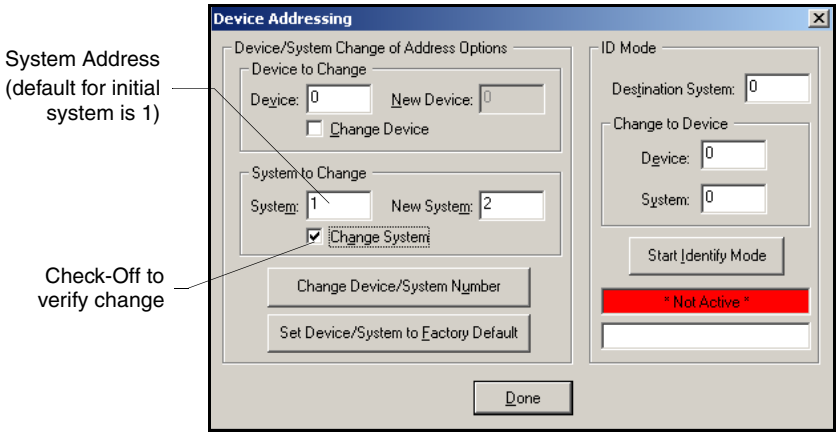


FIG. 18 Device Addressing tab (changing the system value)

NOTE

This tab represents the only way to change the System Number associated to the active Master.

2. Select the **Change System** selection box, from the *System to Change* section.
3. Enter both the current and new system address values (this example uses 2).
4. Click the **Change Device/System Number** button. This configures the Master to accept the new value and incorporate the information. *The system information (in the OnLine Tree tab of the Workspace window) refreshes and then displays the new information.*
5. Click **Done** to close the Device Addressing dialog and return to the main program.
6. Select **Tools** > **Reboot the Master Controller** to access the Reboot the Master dialog, then click **Continue** to reboot the Master and incorporate any changes. Allow 20 - 30 seconds for

the Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

7. Right-click the associated System number and select **Refresh System** to establish a new connection to the specified Master and refresh the System list with devices on that system.
8. Use **Ctrl+S** to save your existing NetLinx Project with the new changes.

NOTE

If the NetLinx device does not appear within the OnLine Tree tab of the Workspace window of NetLinx Studio, make sure that the NetLinx Master System Number (from within the Device Addressing tab) is correctly assigned. ***If there is a problem, use a system value of zero (0) on the NetLinx device.***

NOTE

The Master is default set to DEVICE 0*. Connected NetLinx device addresses can only be changed through the Protected Setup page. The new address is reflected within the OnLine Tree tab of the Workspace window only after the devices are rebooted and the system is refreshed.*

Working with multiple NetLinx Masters

When using more than one Master, each unit must be assigned to a separate System value.

A Master's System value can be changed but its' device Address must always be set to zero (00000). The Device Addressing dialog will not allow you to alter the NetLinx Master address value.

Example: Using NetLinx Studio 2.1 to work with an NXC-ME260 and NI-4000:

- The NXC-ME260 could be assigned to **System 1** (with a value of 00000).
- The NI-4000 could be assigned to **System 2** (with a value of 00000).

Changing the system value on the Modero panel

NOTE

The system value on a Modero touch panel can not be changed from the Device Addressing dialog.

1. Press and hold the grey Front Setup Access button (below the LCD) for **3 seconds** to access the Setup page.
2. Press the **Protected Setup** button to access the Protected Setup page.
3. Use the on-screen keyboard to enter the default password of **1988**.
4. Press the **System Connection** button.
5. Press the blue *System* field on the right of the page to open the Master System Number keypad.
6. Enter the new System value (associated with the Master connected to the panel).
7. Press **Back** to save your changes and return to the Protected Setup page.
8. Press the on-screen **Reboot** button to reboot the panel.
9. Right-click the associated System number (from the **OnLine Tree** tab of the Workspace window) and select **Refresh System** to establish a new connection to the specified Master and refresh the System list with devices on that system.
10. Use **Ctrl+S** to save your existing NetLinx Project with the new changes.

NOTE

If the Master does not appear in the Workspace window, check to make sure that the Master's System Number (from within the Device Addressing tab) is correctly assigned. ***If there is a problem, use a system value of zero (0) on the Master.***

Changing the Device Address on a Netlinx Device

1. Access the Device Addressing dialog (FIG. 19) by either one of these two methods:
   - Right-click on any system device listed in the **OnLine Tree** tab of the Workspace and select **Device Addressing** (from the pop-up list).
   - Select **Diagnostics > Device Addressing** from the Main menu.

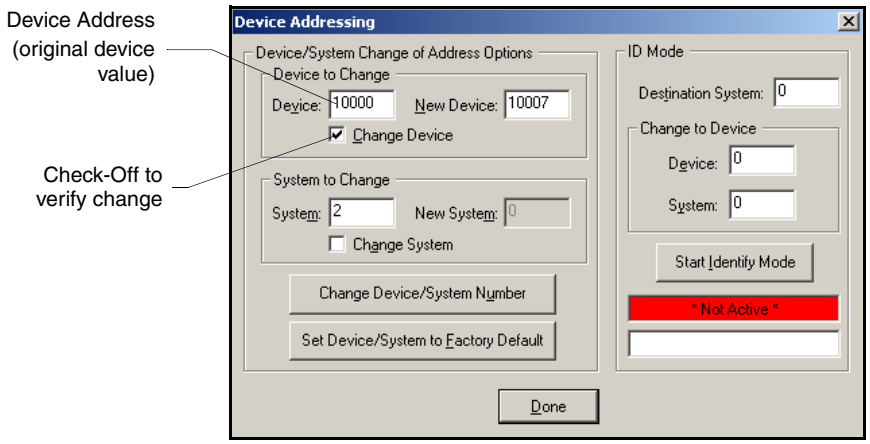


FIG. 19 Device Addressing dialog (changing the device value)

NOTE

This dialog represents the only way to change the device value of a selected NetLinx device (such as a Modero panel).

2. Select the **Change Device** checkbox, from the *Device to Change* section.
3. Enter both the **Current** and **New Device** address values for the target NetLinx device.
4. Click the **Change Device/System Number** button. This configures the specified Master to accept the new value for the NetLinx device and incorporate the information (the system information in the Workspace window refreshes and then displays the new information).
5. Click **Done** to close the Device Addressing dialog.
6. Select **Tools > Reboot the Master Controller** to access the Reboot the Master dialog, then click **Continue** to reboot the Master and incorporate any changes. Allow 20 - 30 seconds for the Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
7. Right-click the associated System number (from the **OnLine Tree** tab of the Workspace window) and select **Refresh System** to establish a new connection to the specified Master and refresh the System list with devices on that system.
8. Use **Ctrl+S** to save your existing NetLinx Project with the new changes.

NOTE

If the Master does not appear in the Workspace window, make sure that the Master's System Number (from within the Device Addressing tab) is correctly assigned. ***If there is a problem, use a system value of zero (0) on the Master.***

Changing the device address on the Modero panel

The device address on a Modero touch panel can not be changed from the Device Addressing dialog. The correct procedure to change a device address is:

1. Press and hold the grey Front Setup Access button (below the LCD on most panels) for **3 seconds** to access the Setup page.
2. Press the **Protected Setup** button to access the Protected Setup page.
3. Use the on-screen keyboard to enter the default password of **1988**.
4. Press the blue *Device Number* field (*this opens a Device Number keypad*).
5. Enter the new Device Address value.
6. Click the **Done** button to close the Device Addressing dialog.
7. Press the on-screen **Reboot** button to reboot the panel.
8. Right-click the associated System number (from the **OnLine Tree** tab of the Workspace window) and select **Refresh System** to establish a new connection to the specified Master and refresh the System list with devices on that system.

Recommended NetLinx Device numbers

• 1 - 255	• Axcess Devices use Axcess standards
• 301 - 3072	• NetLinx CardFrames start at frame number 25 - (frame# * 12) + Card #
• 5001 - 5999	• ICSNet NetLinx devices: NXI, NXM-COM2, NXM-IRS4, etc.
• 6001 - 6999	• ICSNet Landmark devices: PLH-VS8, PLH-AS16, PLB-AS16
• 7001 - 7999	• InConcert Devices
• 8001 - 8999	• PCLink Device: PCLink devices are PC programs
• 10000 - 31999	• ICSNet Panels: DMS, IMS, and future panels
• 33001 - 36863	• Virtual devices: these start at 33001
• 32001 - 32767	• Dynamic devices: the actual range used by Master
• 32768 - 36863	• Virtual devices: the actual range used by Master

Resetting the Factory Default System and Device Values

1. Access the Device Addressing dialog (FIG. 19 on page 23) by either one of these two methods:
   - Right-click on any system device listed in the Workspace and select **Device Addressing**.
   - Select **Diagnostics > Device Addressing** from the Main menu.
2. Click the **Set Device/System to Factory Default** button. This resets both the system value and device addresses (for definable devices) to their factory default settings. The system information (in the **OnLine Tree** tab of the Workspace window) refreshes and then displays the new information.

NOTE

*By setting the system to its default value (#1), Modero panels that were set to connect to the Master on another System value will not appear in the **OnLine Tree** tab of the Workspace window.*
For example: A Modero touch panel was previously set to System #2. The system is then reset to its default setting of System #1 and then refreshed from within the Workspace window. The panel will not reappear until the system is changed (from within the System Connection page on the Modero) to match the new value and both the Master and panel are rebooted.

3. Click **Done** to close the Device Addressing dialog.
4. Select **Tools > Reboot the Master Controller** to access the Reboot the Master dialog, then click **Continue** to reboot the Master and incorporate any changes. Allow 20 - 30 seconds for the Master to reboot.
5. Right-click the associated System number (from the **OnLine Tree** tab of the Workspace window) and select **Refresh Whole Network** to refresh of all project systems, establish a new connection to all Masters, and refresh the System list with devices on that system.
6. Use **Ctrl+S** to save your existing NetLinx Project with the new changes.

Obtaining the Master's IP Address (using DHCP)

NOTE

Verify there is an active Ethernet connection attached to the rear of the Master before beginning these procedures.

1. Select **Diagnostics > Network Addresses** from the Main menu to access the Network Addresses dialog.
2. Verify the **System** number corresponds to the value previously assigned in the Device Addressing tab and verify that zero (0) is entered into the Device field.

NOTE

The system value must correspond to the Device Address entered in the Device Addressing dialog. Refer to the Setting the System Value section on page 21 *for more detailed instructions on setting a system value.*

3. Verify that **NetLinx** appears in the *Host Name* field.
4. Click the **Use DHCP** radio button from the IP Address section (FIG. 20).
5. Click the **Get IP Information** button to read the IP Address obtained by the Master from the DHCP Server and configure the unit for DHCP usage.

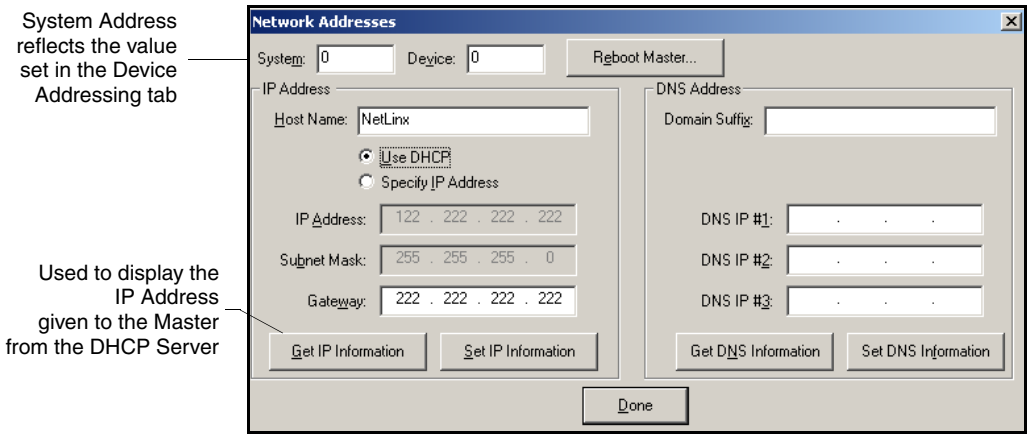


FIG. 20 Network Addresses dialog (showing Get IP)

NOTE

DO NOT enter ANY IP information at this time, this step only gets the System Master to recognize that it should begin using an obtained DHCP Address.

6. Note the obtained IP Address.This information is later entered into the **Master Communication Settings** dialog and used by NetLinx Studio 2.1 (or higher) to communicate to the Master via an IP. This address is reserved by the DHCP server and then given to the Master.

NOTE

If the IP Address field is empty, give the Master a few minutes to negotiate a DHCP Address with the DHCP Server, and try again. The DHCP Server can take anywhere from a few seconds to a few minutes to provide the Master with an IP Address.

7. Click the **Set IP Information** button to retain the IP Address on the Master. A popup window then appears to notify you that Setting the IP information was successful and it is recommended that the Master be rebooted.
8. Click **OK** to accept the new changes.
9. Click the **Reboot Master** button and select **Yes** to close the Network Address dialog. *This process closes the Network Addresses dialog and directs you to the Reboot the Master Controller dialog.*
10. Click **Continue** (*from the Reboot Controller dialog*) and wait for the System Master to reboot and retain the newly obtained DHCP Address. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*

NOTE

*If Studio can not establish communication with the Master, wait a few seconds and click the **Retry** button.*

11. Use **Ctrl+S** to save your existing NetLinx Project with the new changes.
12. Right-click associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system.

Assigning a Static IP to the NetLinx Master

1. Select **Diagnostics** > **Network Addresses** from the Main menu.
2. Verify the **System** number corresponds to the value previously assigned in the Device Addressing tab for the specific System Master.
3. Verify that zero (0) is entered into the **Device** field.

NOTE

The system value must correspond to the Device Address previously entered in the Device Addressing tab. Refer to the Setting the System Value section on page 21 *for more detailed instructions on setting a system value.*

4. Verify that **NetLinx** appears in the Host Name field.
5. Click the **Specify IP Address** radio button from the IP Address section (FIG. 21).

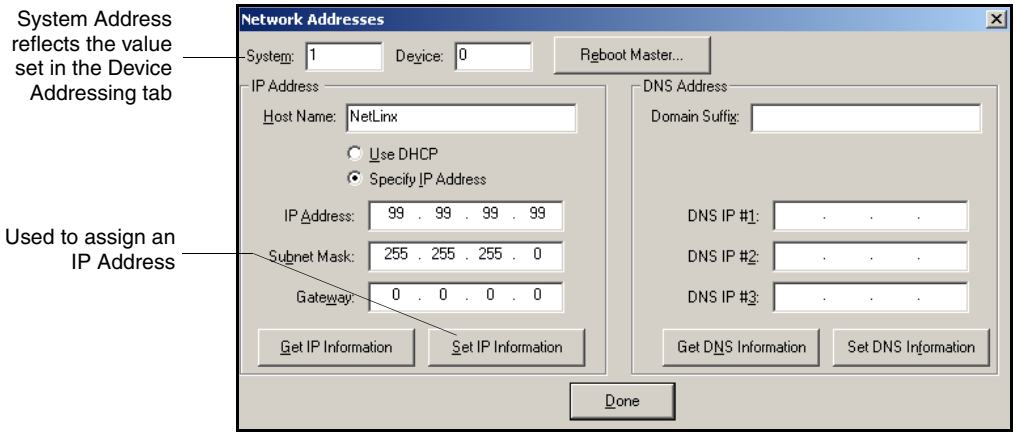


FIG. 21 Network Addresses dialog (showing Set IP)

6. Enter the IP Address, Subnet Mask, and Gateway information into their respective fields.
7. Click the **Set IP Information** button to retain a known IP Address (obtained from the System Administrator) on the specified System Master.
8. Click **OK** to accept the new changes.
9. Click the **Reboot Master** button and select **Yes** to close the Network Address dialog. *This process closes the Network Addresses dialog and directs you to the Reboot the Master Controller dialog.*
10. Click **Continue** (*from the Reboot controller dialog*) and wait for the System Master to reboot and incorporate the newly obtained DHCP Address. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
11. Right-click associated System number and select **Refresh System**. This establishes a new connection to the specified System and populates the list with devices on that system.

NOTE

Verify that these IP values are also entered into the related fields within either the IP Settings section of the System Connection page (on the touch panel) or within the Address field on the web browser.

Communicating with the NetLinx Master via an IP

Whether the Master's IP Address was Set (Set IP Info) or obtained (Get IP Info), use the information from the Network Addresses dialog to establish a new communication method to the Ethernet connected Master.

1. Launch NetLinx Studio 2.1 (default location is **Start > Programs > AMX Control Disc > NetLinx Studio > NetLinx Studio 2.1**).
2. Obtain the IP Address of the Master from your System Administrator, if you do not have an IP Address:
   - Follow the steps outlined in either the *Obtaining the Master's IP Address (using DHCP)* section on page 25 or *Assigning a Static IP to the NetLinx Master* section on page 27.
3. Select **Settings > Master Communication Settings**, from the Main menu to open the Master Communication Settings dialog (FIG. 22).

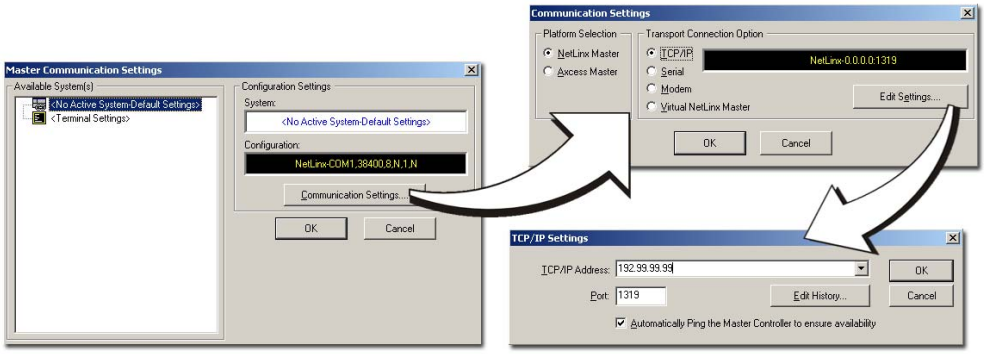


FIG. 22 Assigning Communication Settings and TCP/IP Settings

4. Click the **Communications Settings** button to open the Communications Settings dialog.
5. Click on the **NetLinx Master** radio button (*from the Platform Selection section*) to indicate that you are working with a NetLinx Master (such as the NXC-ME260 or NI-Series of Integrated Controllers).
6. Click on the **TCP/IP** radio button (*from the Transport Connection Option section*) to indicate you are connecting to the Master through an IP Address.
7. Click the **Edit Settings** button (*on the Communications Settings dialog*) to open the TCP/IP Settings dialog (FIG. 22).
8. Enter the IP Address into the *TCP/IP Address* field. This information is obtained from either your System Administrator or from the *Obtaining the Master's IP Address (using DHCP)* section on page 25.
9. Click **OK** three times to close the open dialogs and save your settings.

NOTE

If you are currently connected to the assigned Master, a popup asks whether you would want to temporarily stop communication to the Master and apply the new settings.

10. Click **Yes** to interrupt the current communication from the Master and apply the new settings.

11. Select **Tools > Reboot the Master Controller** to access the Reboot the Master dialog, then click **Continue** to reboot the Master and incorporate any changes. Allow 20 - 30 seconds for the Master to reboot. *The STATUS and OUTPUT LEDs should begin to alternately blink during the incorporation. Wait until the STATUS LED is the only LED to blink.*
12. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
13. Right-click the *Empty Device Tree/System* entry and select **Refresh System** to establish a new connection to the System's Master and refresh the list with online system devices. *The communication method is then highlighted in green on the bottom of the NetLinx Studio window.*

NOTE

If the connection fails to establish, a Connection Failed dialog appears.
Try selecting a different IP Address if communication fails.
*Press the **Retry** button to reconnect using the same communication parameters.*
*Press the **Change** button to alter your communication parameters and repeat steps 2 thru 10.*

14. Once the particular System Master is configured for communication via an IP Address, remove the RS232 connector from the Program port on the NetLinx Master.

Installing New NetLinx Master Firmware via an IP

1. Click the **OnLine Tree** tab in the Workspace window to view the devices on the System. *The default System value is one (1).*
2. Right-click on the *Empty Device Tree/System* entry and select **Refresh System** to establish a new connection to the System's Master and refresh the list with online system devices.
3. After the Communication Verification dialog window verifies active communication between the PC and the Master, verify the NetLinx Master appears in the **OnLine Tree** tab of the Workspace window (FIG. 23).

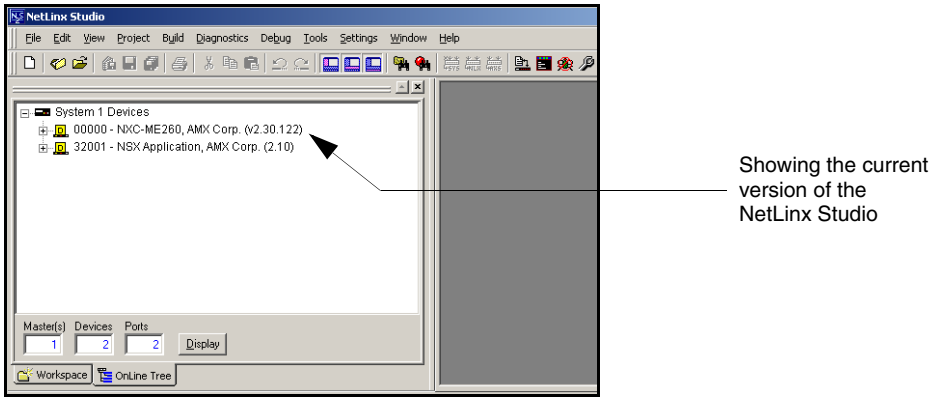


FIG. 23 Initial NetLinx Workspace window (showing the OnLine Tree tab)

NOTE

The current firmware version of the Master is displayed to the right of the device.

4. If the firmware version is not **build 139** (v2_XX_**139**) for the NXC-ME260; locate the latest firmware file from **www.amx.com > Tech Center > Downloadable Files > Firmware Files > NetLinx Masters**.
5. Verify you have downloaded the latest Master firmware (KIT) file to a known location.
6. Select **Tools > Firmware Transfers > Send to NetLinx Device** from the Main menu to open the Send to NetLinx Device dialog (FIG. 24). Verify the target's System number matches the value listed within the active System folder in the **OnLine Tree** tab of the Workspace.

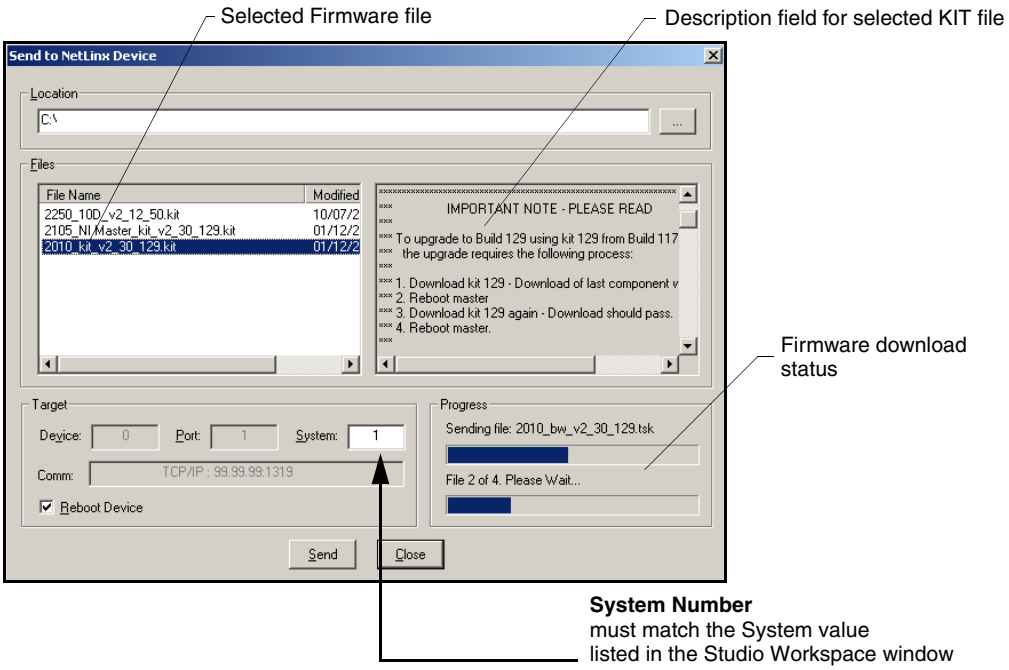


FIG. 24 Select to NetLinx Device dialog (showing Master firmware update via IP)

7. Select the Master's KIT file from the **Files** section (FIG. 24).

NOTE

*The KIT file for the **ME260** begins with **2010_kit** (the KIT file for the NI-Series of Master controllers begins with 2105_NI Master).*

8. Enter the **System** number associated with the target Master (*listed in the OnLine Tree tab of the Workspace window*). *The Device and Port fields are greyed-out.*
9. Click the **Reboot Device** checkbox to reboot the Master after the firmware update process is complete.
10. Click **Send** to begin the transfer. The file transfer progress is indicated on the bottom-right of the dialog (FIG. 24).

NOTE

***Only upon the initial installation** of the new **build 139** KIT file to a Master there will be a failure of the last component to successfully download. This is part of the initial update procedure and will not occur during uploads of later firmware.*

11. After the last components fails to install, click Close and reboot the Master by selecting **Tools > Reboot the Master Controller > Continue** to begin the process.

12. Repeat steps 8 - 11 again (the last component will successfully be installed).
13. Click **Close** once the download process is complete.

The OUTPUT and INPUT LEDs alternately blink to indicate the Master is incorporating the new firmware. Allow the Master 20 - 30 seconds to reboot and incorporate the new firmware.

14. Right-click on the *System* entry and select **Refresh System**. This establishes a new connection to the System and populates the list with devices on your system.

NetLinx Security and Web Server

NetLinx ME260 Masters (installed with firmware **build 139** incorporate new built-in security and SSL certificate verification capabilities. By using both SSL certificate verification and secured HTTP access, this new NetLinx firmware provides users with a more convenient web-based method of securing both the Master and the incoming and outgoing information.

Terminal setup and security configuration is still valid and supported in the new build of NetLinx Master firmware. New Terminal security features include the use of two new commands: `ssl security enable` and `ssl security disable`.

SSL (*Secure Sockets Layer*) is a protocol that works by encrypting data that is transferred over the SSL connection. URLs that require an SSL connection begin with **https:** instead of **http:** in the browser's Address field. These security capabilities are configured to function via a web session within your browser.

NOTE

*After the installation of **build 139** to your Master, Telnet security configuration access is disabled. This new build migrates the NetLinx Master security setup from a TELNET environment to a web-based application.*

The new NetLinx Web Server used to power the Master security and SSL certificate features on AMX Masters, not only provides user name/password security for the target Master, but also a new level of secure encryption through the use of a unique server certificate.

The first layer of security for the Master is an on-screen HTTP user name and password field that prompts a user to provide correct security information before gaining access to a target Master. The second layer of protection is an SSL Certificate (specifically identifying the target Master) that can either be requested or self-generated. This certificate is then installed onto the target Master and added to the trusted site certificate listing within the computer's Internet browser.

NetLinx Security web browser and feature support

The following table describes the web browsers (associated to each operating system) recommended for use with the new NetLinx Security features on the NXC-ME260.

Supported Browser and Feature Compatibility

OS Platform	Recommended Browser	NetLinx Security Feature support	G3 Web Panel Control support	G4 Web Panel Control support
Windows©	**Internet Explorer®** 6.0 or higher	**Yes**	**Yes** *Sun Java must be installed*	**Yes**
MAC©	**Safari®** *- (see note below)*	**Yes**	**Yes**	**No**
Linux©	**Mozilla®**	**Yes** *- (see note below)*		

NOTE

When using Safari on a MAC machine, certificates must be externally requested from the Server Certificate's page. Self-generated certificates do not allow access back to the target Master and will display an invalid certificate message.

NOTE

When using Mozilla on a Linux machine, the Group Rights column checkboxes (from within the Modify User page) can become greyed-out but are actually present.

New Master Firmware Security Features

- **Master Security**
- **Telnet Security**
- **Terminal (RS232 Program port) security**
- **HTTP (Web Server) Security**
- **FTP Security**
- **SSL Certificate Encryption and Identification Technology**

NOTE

Installation of this new SSL functionality onto your Master will cause security setup via Telnet to be disabled. *Although Telnet security configuration access can no longer be used with the Master, a Terminal connection (using HyperTerminal) can still be established using the Master's RS232 Program port. Refer to the NetLinx Security with a Terminal Connection* section on page 73 *for detailed Terminal security setup procedures.*

The migration from a Telnet session to the use of an HTTP web browser allows a user to fully utilize the latest SSL encryption features available within the newest release of NetLinx Master firmware.

NetLinx Security Terms

The following table lists those commonly used NetLinx Security terms:

NetLinx Security Terms	
User	A user is a single potential client of the NetLinx Master.
Administrator	An administrator has privileges to modify existing NetLinx Master access groups, users, and their rights. The administrator can also assign NetLinx communication access rights for different users or groups (ex: Telnet and HTTP access) and configure the SSL server certificate.
Group	A group is a logical collection of users. Note that any properties possessed by groups (ex: access rights, directory associations, etc.) are inherited by all of the members of the group.
User name	A user name is a valid character string (4 - 20 alpha-numeric characters) defining the user. This string is ***case sensitive***. Each user name must be unique.
Group name	A group name is a valid character string (4 - 20 alpha-numeric characters) defining the group. This string is ***case sensitive***. Each group name must be unique.
Password	A password is a valid character string (4 - 20 alpha-numeric characters) to supplement the user name in defining the potential client. This string is also ***case sensitive***.
Access Rights	Each of the NetLinx Master features has security procedures defined for them. The access right for a particular feature determines if the user or group will have access to the feature.

NetLinx Security Terms (Cont.)	
Directory Associations	A Directory Association is a path that defines the directories or files a particular user or group can access via the Web Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is ***case sensitive***. This is the path to the file or directory you want to grant access.

Accessing the NetLinx Master via an IP Address

Refer to the *Installing New NetLinx Master Firmware via an IP* section on page 29 for more detailed information on how to download the latest firmware (**build 139**) from **www.amx.com**. This firmware build enables SSL security and disables the ability to alter the Master security properties via a TELNET session.

NOTE

Although Telnet security configuration access can no longer be used with the Master, a Terminal connection (using HyperTerminal) can still be established using the Master's RS232 Program port.

Once the Master's IP Address has been set through NetLinx Studio (version 2.1 or higher):

1. Launch your web browser.
2. Enter the IP Address of the target Master (***ex: 198.198.99.99***) into the web browser's *Address* field.
3. Press the Enter key on your keyboard to begin the communication process between the target Master and your PC.
4. Click **OK** to accept the AMX SSL certificate (*if SSL is enabled*).
5. The first tab displayed within your open browser window is WebControl.

WebControl Tab

This tab (FIG. 25) displays links to both G3 web panel pages downloaded to the target Master and G4 panels running the latest G4 Web Control feature. **G3 can't be controlled with firmware greater than 139. The ME260 cannot use firmware greater then 139.**

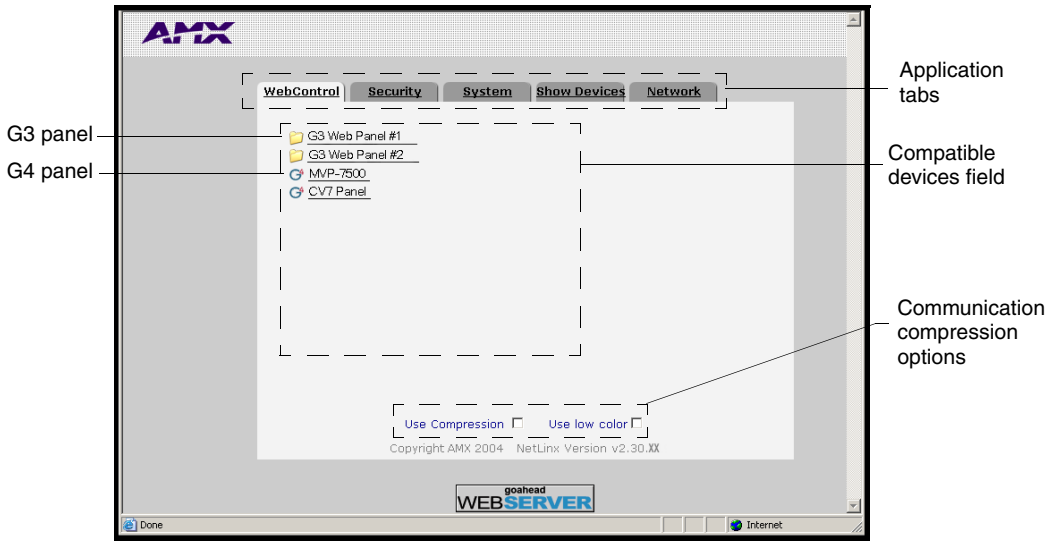


FIG. 25 WebControl Tab (populated with panels)

NOTE

G3 panel pages accessed through the WebControl tab are virtual pages created by a user in TPDesign3 and then downloaded to the target Master. Interaction with these pages are not reflected on an actual G3 panel unless you use specific programming commands that link these virtual pages with their real G3 panel counterparts.

The following table lists the WebControl tab features that an administrator or other authorized user can select from:

WebControl Tab Features	
Feature	**Description**
Compatible Devices Field	This area displays: • Links to G3 user designed web panels (containing an index.htm page) that are installed on the NetLinx Master. • G4 icons (with associated links) if a G4 panel running Web Control is communicating with the target Master.
Communication Compression Options	Allows you to choose from among two compression options: • **These compression settings are most useful when working over a bandwidth-restricted network or over the Internet.** • **Use Compressio**n allows the user to specify that the transmitted data packets be compressed. This speeds up the visual responses from the panel by minimizing the size of the information relayed through the web and onto the PC screen. • **Use Low Color** allows the user to specify the number of colors used to display the image from the panel be reduced. By reducing the numbers of colors used to display the panel page on the PC, the size of the information is reduced, and the response delay is decreased.

Default Security Configuration

By default, the NetLinx Master will create the following accounts, access rights, directory associations, and security options:

Default Security Configuration		
Account 1	**Account 2**	**Group 1**
User name: administrator	User name: NetLinx	Group: administrator
Password: password	Password: password	Rights: All
Group: administrator	Group: none	Directory Association: /*
Rights: All	Rights: FTP Access	
Directory Association: /*	Directory Association: none	

Security Options: **FTP Security - Enabled**
Admin Change Password Security - Enabled
All other options - Disabled

NOTE

SSL security is disabled by default. If the user/group is given FTP access rights by the administrator, all directories can become accessible (read/write/modify).

- The ***administrator*** user account cannot be deleted or modified with the exception of its password. Only a user with "Change Admin Password Access" rights can change the administrator password.

- The ***NetLinx*** user account is created to be compatible with previous NetLinx Master firmware versions. This account is initially created by default and can later be deleted or modified.
- The ***administrator*** group account cannot be deleted or modified.
- The FTP Security and Admin Change Password Security are always enabled and cannot be disabled.

NOTE

Internet Explorer is used for the purposes of these instructions. Refer to the Table , "Supported Browser and Feature Compatibility," on page 33 for browser and OS compatibility information.

Security Tab

NetLinx system security allows you to define access rights for users or groups.

The Enable/Disable Security features (FIG. 26) are only displayed after the left Enable Security link is selected.

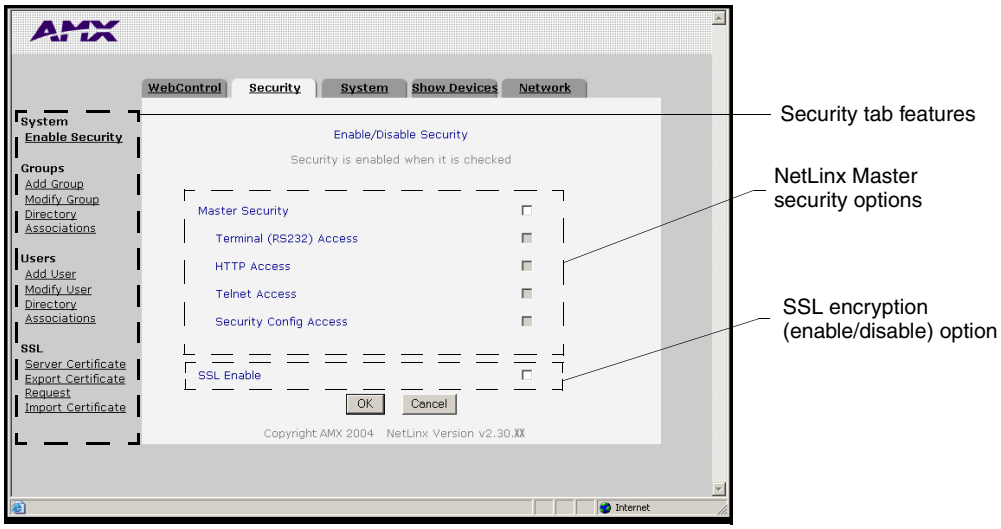


FIG. 26 Security Tab - Enable/Disable Security

The following table lists the NetLinx System Security Enable or Disable options that an administrator or other authorized user can grant or deny access to:

Security Tab Features	
Feature	**Description**
System section	Provides an authorized user with the ability to alter the current security options assigned to the target Master.
Groups section	Provides an authorized user with the ability to alter group properties such as creating a group, modifying an existing groups' rights, and define the files/directories accessible by a particular group. • Any properties possessed by a group (access rights/directory associations, etc.) are inherited by all members of that group.
Users section	Provides an authorized user with the ability to alter user properties such as creating a user, modifying an existing users' communication rights, and defining the files/directories accessible by a particular user.

Security Tab Features (Cont.)	
SSL Certificate section	Allows an authorized user to select the method for SSL certificate generation and implementation on the target Master. • A certificate can be self generated, requested, or regenerated. • Once a certificate has been installed onto a target Master, that certificate remains there until it is either replaced or regenerated.

Security tab - Enable Security page

It is recommended that enabling the Master Security option be done after the groups, users, and passwords have been setup. If not, when the user accesses the Master from within another session, the default administrator user names and password are used for access.

The **Enable Security** link toggles the appearance of the NetLinx Master security options.

Security System Features	
Feature	**Description**
Master Security Configuration	This option allows an authorized user the ability to grant/deny access to the security configuration commands of the on-board Master. Only those users with security access rights granted will have access to the security configuration commands. • These are global options that enable or disable the rights given to both users and groups. • Ex: If you would want to disable Telnet Security for all users, you would access this tab and uncheck the Telnet Access option to disable Telnet security for the entire Master.
Terminal (RS232) Security	This selection enables or disables Terminal Security (through the RS232 Program port). If Terminal Security is enabled, a user must have sufficient access rights to login to a Terminal session.
HTTP Access	This selection enables or disables Web Server access. If Security is enabled, a user must have sufficient access rights to browse to the NetLinx Master with a Web Browser. • **Enabling this field prompts the user (upon their return) to submit a valid user name and password.**
Telnet Access	This selection enables or disables Telnet Security. If Telnet Security is enabled, a user must have sufficient access rights to login to a Telnet session.
Security Config Access	This selection enables or disables the ability of a group to alter the Security Configuration settings. If Security Configuration Security is enabled, a user/group must have sufficient access rights to access the Main Security Menu.
SSL Enable	This option allows an administrator the ability to enable or disable the SSL feature on the Master. • **This field will not be enabled until after the initial self-generated certificate has been installed onto the Master. This configures the Master for secure communication. This security is necessary before installing any encrypted CA server certificates.** • **If the self-generated SSL certificate has been installed on the Master, the user is prompted with a Security Alert popup that informs them of possible conflicts between the Master's certificate and those registered through the web browser as valid and secure. Refer to the *Accessing an SSL-Enabled Master via an IP Address* section on page 68 for more information.**

Security System Features (Cont.)	
OK/Cancel	• Press **OK** to accept any changes made within this tab and incorporate the information into the target Master. • Press **Cancel** to void any changes made within this tab, exits without making changes to the target Master, and blanks-out the Security tab.

NOTE

*You must first enable the Master Security selection and then click **OK** before altering any settings.*
*Click **OK** again after making alterations to any of these features (such as Terminal, HTTP, and Telnet access) and save these changes to the target Master.*

Security tab - Add Group page

The **Groups** > **Add Group** link allows an authorized user to add a group account (FIG. 27) and then assign that group's current Master access rights.

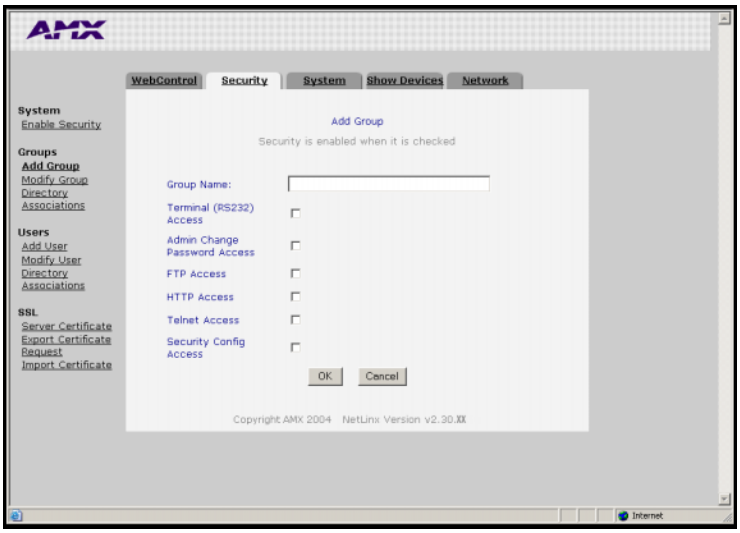


FIG. 27 Security Tab - Add Group

Add Group Entries	
Feature	**Description**
Group Name	A valid character string defining the name of the group (4 - 20 alpha-numeric characters). • The string is case sensitive and must be unique.
Terminal (RS232) Access	This selection enables or disables Terminal (RS232 Program port) Security Access for the target group.
Admin Change Password Access	This selection enables or disables the group's right to change the administrator's user passwords. ***Note:*** Once the Administrator's password has been changed, the default password can no longer be used to gain access.
FTP Access	This selection enables or disables FTP Access for the target group.
HTTP Access	This selection enables or disables Web Server access for the target group.
Telnet Access	This selection enables or disables Telnet Security access for the target group.
Security Config Access	This selection enables or disables the ability of a group to alter the Security Configuration settings.

Add Group Entries (Cont.)	
OK/Cancel	• Press **OK** to accept any changes made within this tab and incorporate the information into the target Master. • Press **Cancel** to void any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab.

NOTE

*A **User** represents a single potential client of the NetLinx Master, while a **Group** represents a logical collection of users. Any properties possessed by groups (example: access rights, directory associations, etc.) are inherited by all the members of the group.*

Security tab - Modify Group page

The **Groups** > **Modify Group** link allows an authorized user to select from a listing of available groups (FIG. 28) and then modify the access rights for the selected group.

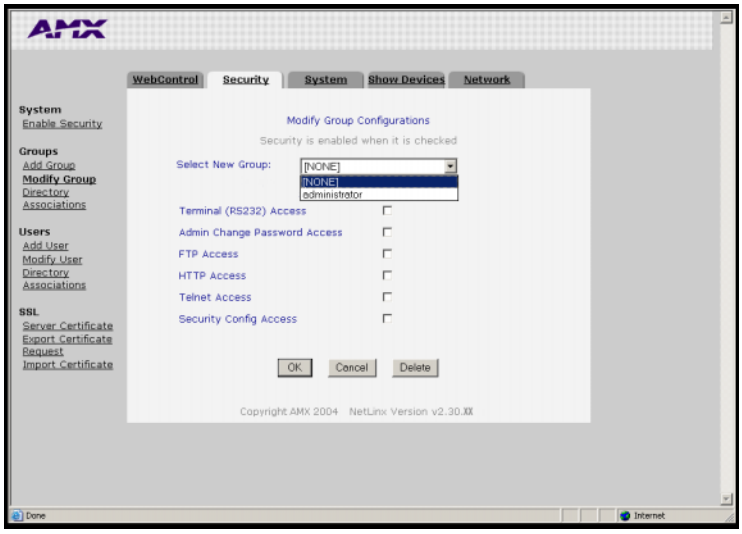


FIG. 28 Security Tab - Modify Group

Modify Group Entries	
Feature	**Description**
Select New Group	Provides a drop-down listing of the available groups. • Initially, administrator is listed as a default group. Thereafter, the last group accessed is then always shown. • As more groups are added through the **Add Group** section of the Security tab; those groups appear within the drop-down selection. • The checkbox for each access right is populated when a new group is selected.
Terminal (RS232) Access	This selection enables or disables Terminal Security Access (through the RS232 Program port) for the selected group.
Admin Change Password Access	This selection enables or disables the group's right to change the administrator's user passwords. ***Note:*** Once the Administrator's password has been changed, the default password can no longer be used to gain access.
FTP Access	This selection enables or disables FTP Access for the selected group.

Modify Group Entries (Cont.)	
HTTP Access	This selection enables or disables Web Server access for the selected group.
Telnet Access	This selection enables or disables Telnet Security for the selected group.
Security Config Access	This selection enables or disables the ability of a group to alter the Security Configuration settings.
OK/Cancel/Delete	• Press **OK** to accept any changes made within this tab and incorporate the information into the target Master. • Press **Cancel** to void any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab. • Press **Delete** to remove the selected group from the list of authorized groups on the Master.

Security tab - Group Directory Associations page

The **Groups > Directory Associations** link allows an authorized user to view current directory associations assigned to the selected group, add paths for new directory associations, and delete any previously configured directory associations (FIG. 29).

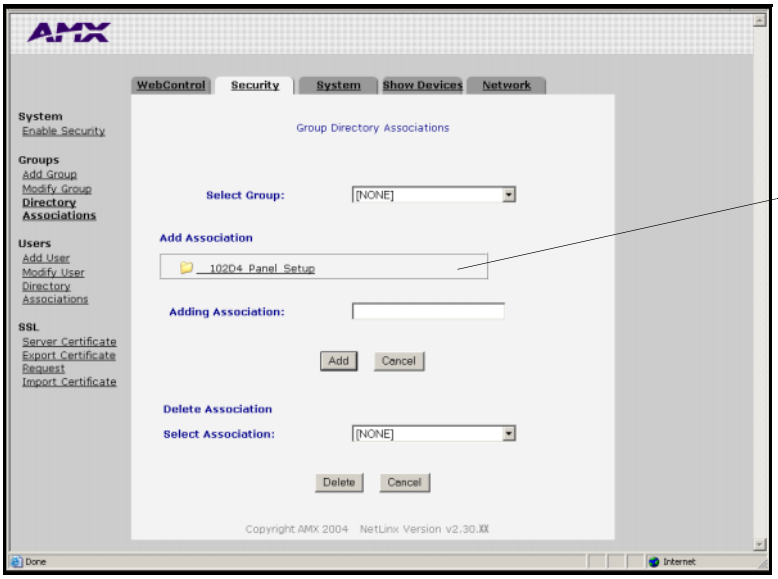


FIG. 29 Security Tab - Group Directory Associations

A Directory Association is a path that defines the directories and files a particular user or group can access via the Web Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is ***case sensitive***. This is the path to the file or directory to which you want to grant access.

A single '/' is sufficient to grant access to all files and directories in the user directory and subdirectory. The '/*' wildcard can also be added to enable access to all files. All entries should start with a '/'.

Here are some examples of valid entries:

Valid Directory Association Entries	
Path	**Description**
/	Enables access to the all files within the user's main directory and subdirectories.
/*	Enables access to the all files within the user's main directory and subdirectories.
/user1	If user1 is a file in the user directory, only the file is granted access. If user1 is a subdirectory of the user directory, all files in the user1 and its sub-directories are granted access.
/user1/	user1 is a subdirectory of the user directory. All files in the user1 and its sub-directories are granted access.
/Room1/iWebControlPages/*	/Room1/iWebControlPages is a subdirectory and all files and its subdirectories are granted access.

By default, all accounts that enable HTTP Access are given a '/*' Directory Association if no other Directory Association has been assigned to the account.

Group Directory Association Entries	
Feature	**Description**
Select New Group	Provides a drop-down listing of the available groups. • Initially, administrator is listed as a default group. Thereafter, the last group accessed is then always shown. • As more groups are added through the **Add Group** section of the Security tab; those groups appear within the drop-down selection. • The checkbox alongside each access right is populated when a new group is selected.
Add Association	This field displays all existing directories currently on the target Master. • These folders can consist of G3 HTML project folders, data file folders, etc. • These folders are located beneath the User directory on the Master.
Adding Association	This field is used to specify the path for the file or directory granted for access and then assigned to the selected group. • Clicking on a folder within the Add Association area populates the Adding Association association field with the folder's path. • The directory path can also manually be entered. • Press **Add** to accept the new path and assign it to the selected group. • Press **Cancel** to void any path changes.
Delete/Select Association	This drop-down listing displays any current directory associations assigned to the group and prompts you to select the association you want to delete. • Press **Delete** to remove the currently selected directory association and save those changes to the group profile. • Press **Cancel** to void any association changes.

Security tab - Add User page

The **Users** > **Add User** link allows an authorized user to add a user account (FIG. 30) and then assign that user's current access rights.

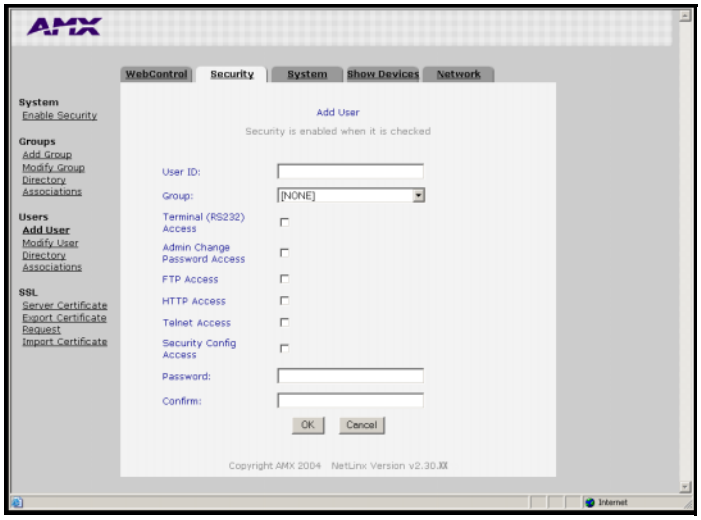


FIG. 30 Security Tab - Add User

Add User Entries	
Feature	**Description**
User ID (user name)	A valid character string defining the name of the user (4 - 20 alpha-numeric characters). The string is case sensitive and must be unique.
Group	Provides a drop-down listing of the available groups. • Any properties possessed by groups (ex: access rights, directory associations, etc.) are inherited by users assigned to a particular group.
Terminal (RS232) Access	This selection enables or disables Terminal Security Access (through the RS232 Program port) for the target user.
Admin Change Password Access	This selection enables or disables the user's right to change the administrator's user passwords. ***Note:*** Once the Administrator's password has been changed, the default password can no longer be used to gain access.
FTP Access	This selection enables or disables FTP Access for the target user.
HTTP Access	This selection enables or disables Web Server access for the target user.
Telnet Access	This selection enables or disables Telnet Security access for the target user.
Security Config Access	This selection enables or disables the ability of a user to alter the Security Configuration settings.
Password/Confirm	Enter a password for the new user. • A user password is a valid character string (4 - 20 alpha-numeric characters) that is used to supplement the user name/ID in defining the potential client. The string is case sensitive and must be unique.
OK/Cancel	• Press **OK** to accept any changes made within this tab and incorporate the information into the target Master. • Press **Cancel** to void any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab.

Security tab - Modify User page

The **Users** > **Modify User** link allows an authorized user to select from a listing of available users (FIG. 31) and then modify the Master's access rights for the selected user.

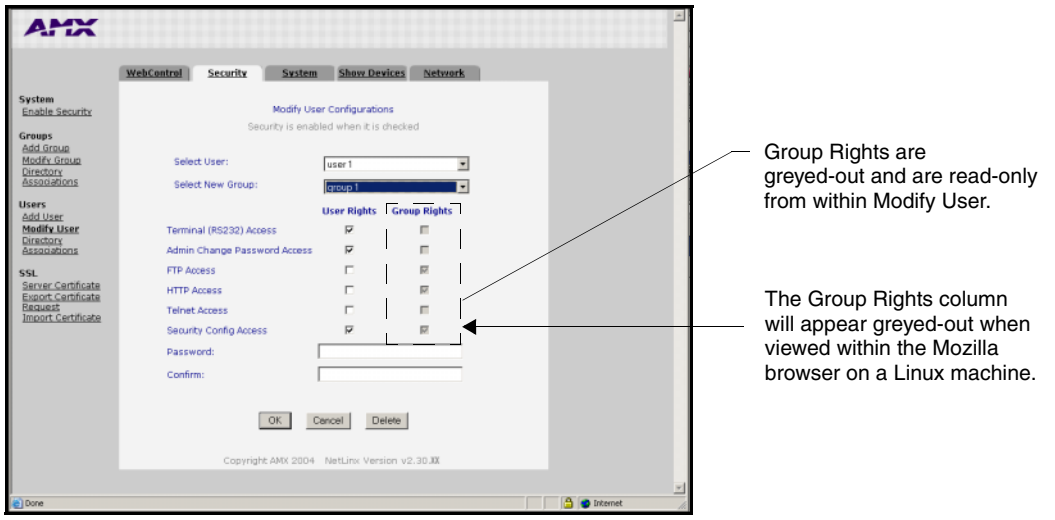


FIG. 31 Security Tab - Modify User

Modify User Entries	
Feature	**Description**
Select User	Provides a drop-down selection listing of the available users. • Initially, *administrator* and *NetLinx* are listed as a default users. The *administrator* has **ALL** available group and User access rights. The *NetLinx* user has only FTP user rights and no pre-assigned group rights. Thereafter, the last user accessed is then always shown. • As more users are added through the **Add User** section of the Security tab; those users appear within the drop-down selection (along with checkmarks alongside their selected user access rights).
Select New Group	Provides a drop-down selection listing of the available groups. • As more groups are added through the **Add Group** section of the Security tab; those groups appear within the drop-down selection (along with their directory associations). • Any properties possessed by groups (ex: access rights, directory associations, etc.) are inherited by users assigned to a particular group.
Terminal (RS232) Access	This selection enables or disables Terminal access (through the RS232 Program port) for the selected user.
Admin Change Password Access	This selection enables or disables the user's right to change the administrator's user passwords. ***Note:*** Once the administrator's password has been changed, the default password can no longer be used to gain access.
FTP Access	This selection enables or disables FTP Access for the selected user.
HTTP Access	This selection enables or disables Web Server access for the selected user.

Modify User Entries (Cont.)	
Telnet Access	This selection enables or disables Telnet access for the selected user.
Security Config Access	This selection enables or disables the ability of a user to alter the Security Configuration settings.
Password/Confirm	Enter a new password assigned to the selected user. • A user password is a valid character string (4 - 20 alpha-numeric characters). **The string is case sensitive and must be unique.** • If this field is left blank the current password is left unchanged. • If a new alpha-numeric string is entered, it becomes incorporated as the new password after pressing the **OK** button.
OK/Cancel/Delete	• Press **OK** to accept any changes made within this tab and incorporate the information into the target Master. • Press **Cancel** to void any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab. • Press **Delete** to remove the selected user from the list of authorized users on the Master.

Security tab - User Directory Associations page

The **Users > Directory Associations** link allows an authorized user to view current directory associations assigned to the selected user, add paths for new directory associations, and delete any previously configured directory associations (FIG. 32).

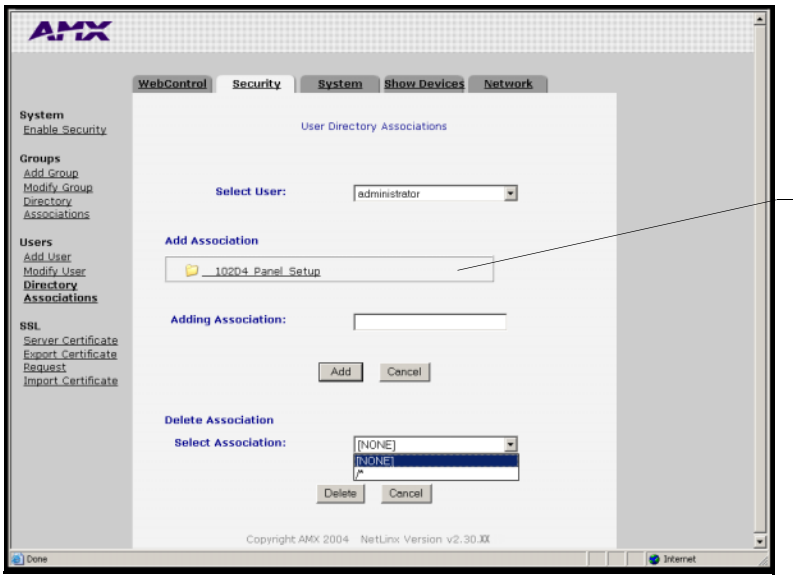


FIG. 32 Security Tab - Group Directory Associations

A Directory Association is a path that defines the directories and/or files a particular user or group can access via the Web Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is ***case sensitive***. This is the path to the file or directory to which you want to grant access.

A single '/' is sufficient to grant access to all files and directories in the user directory and it's subdirectory. The '/*' wildcard can also be added to enable access to all files. All entries should start with a '/'. Here are some examples of valid entries:

Valid Directory Association Entries

Path	Description
/	Enables access to the user directory and all files and subdirectories in that user directory.
/*	Enables access to the user directory and all files and subdirectories in that user directory.
/user1	If user1 is a file in the user directory, only the file is granted access. If user1 is a subdirectory of the user directory, all files in the user1 and its sub-directories are granted access.
/user1/	user1 is a subdirectory of the user directory. All files in the user1 and its sub-directories are granted access.
/Room1/iWebControlPages/*	/Room1/iWebControlPages is a subdirectory and all files and its subdirectories are granted access.

By default, all accounts that enable HTTP Access are given a '/*' Directory Association if no other Directory Association has been assigned to the account.

User Directory Association Entries

Feature	Description
Select User	Provides a drop-down listing of the available users. • Initially, *administrator* and *NetLinx* are listed as default users. Thereafter, the last user accessed is then always shown. • As more users are added through the **Add Group** section of the Security tab; those users appear within the drop-down selection. • The checkbox alongside each access right is populated when a new user is selected.
Add Association	This field displays all existing directories currently on the target Master. • These folders can consist of G3 HTML project folders, data file folders, etc. • These folders are located beneath the User directory on the Master.
Adding Association	This field is used to specify the path for the file or directory granted for access and then assigned to the selected user. • Clicking on a folder within the Add Association area populates the Adding Association association field with the folder's path. • Another field option is to manually enter the directory path. • Press **Add** to accept the new path and assign it to the selected user. • Press **Cancel** to void any path changes.
Delete/Select Association	This drop-down listing displays any current directory associations assigned to the user and prompts you to select the association you want to delete. • Press **Delete** to remove the currently selected directory association and save those changes to the user profile. • Press **Cancel** to void any path changes, disables the security configuration session, and returns you to a blank Security tab.

Security tab - SSL Server Certificate page

A certificate is a cryptographically signed object that associates a public key and an identity. Certificates also include other information in extensions such as permissions and comments. A "**CA**" is short for Certification Authority and is an internal entity or trusted third party that issues, signs, revokes, and manages these digital certificates.

CAUTION

***Before initially enabling the SSL feature on the Master**, a self-generated certificate must first be installed. This initial installation allows users to then later install the different types of certificates (requested, self-generated, or regenerated).*

The **SSL > Server Certificate** link (FIG. 33) allows an authorized user to display an installed certificate, create a certificate request, self-generate, and regenerate SSL Server Certificates.

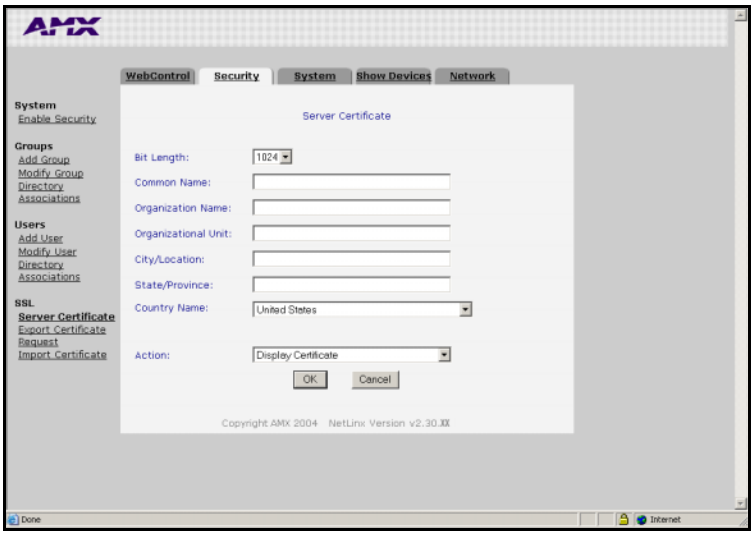


FIG. 33 Security Tab - Server Certificate

Server Certificate Entries	
Feature	**Description**
Bit Length	Provides a drop-down selection with three available public key lengths: 512, 1024, and 2048. • Longer key lengths result in increased certificate processing times. • A longer key length results in more secure certificates.
Common Name	The Common Name of the certificate MUST be the URL Domain Name used. • Example: If the address used is www.amxuser.com, that must be the Common name and format used. • **The Common Name can not be an IP Address.** • If the server is internal, the Netbios name must be used. • For every website using SSL that has a distinct DNS name, there must be a certificate installed. Each website (external or Internet) for SSL MUST also have a distinct IP Address.
Organization Name	Name of your business or organization. This is an alpha-numeric string (1 - 50 characters in length).
Organizational Unit	Name of the department using the certificate. This is an alpha-numeric string (1 - 50 characters in length).

Server Certificate Entries (Cont.)	
City/Location	Name of the city where the certificate is used. This is an alpha-numeric string (1 - 50 characters in length).
State/Province	Name of the state or province where the certificate is used. This is an alpha-numeric string (1 - 50 characters in length).
Country Name	Provides a drop-down selection with a listing of currently selectable countries.
Action	Provides a drop-down selection with a listing of available certificate options: • Display Certificate - Populates the Server Certificate fields with the information from the certificate currently installed on the Master. ***This action is used only to display the information contained in the certificate on the target Master.*** • Create Request - Takes the information entered into the previous fields and formats the certificate so it can be exported to the external Certificate Authority (CA) for later receipt of an SSL Certificate. ***This action is used to request a certificate from an external source.*** • Self Generate Certificate - Takes the information entered into the previous fields and generates its own SSL Certificate. ***This action is used when no previous certificate has been installed on the target Master, or a self-signed certificate is desired.*** • Regenerate Certificate - Takes the information entered into the previous fields and regenerates an SSL Certificate. This action changes the Master Key. ***This method of certificate generation is used to modify or recreate a previously existing certificate already on the Master.***
OK/Cancel/Delete	• Press **OK** to accept any changes made within this tab and incorporate the information into the target Master. • Press **Cancel** to void any changes made within this tab, disable the security configuration session, void any changes made to the Master, and return you to the empty Security tab.

CAUTION

*If a certificate has been purchased from an external CA and then installed onto a specific Master, **DO NOT regenerate the certificate** or alter its properties (ex: bit length, city, etc.).*
If the purchased certificate is regenerated, it becomes invalid.

A certificate consists of two different Keys:

- **Master Key** is generated by the Master and is incorporated into the text string sent to the CA during a certificate request. It is unique to a particular request made on a specific Master.
- **Public Key** is part of the text string that is returned from the CA as part of an approved SSL Server Certificate. This public key is based off the submitted Master key from the original request.
- **Regenerating a previously requested and installed certificate invalidates that certificate because the Master Key has been changed.**

Security tab - Export Certificate Request page

The **SSL > Export Certificate Request** link opens an Export Certificate Request field (FIG. 34) where an authorized user can copy the raw text from a generated Certificate request into their clipboard and then send it to the CA.

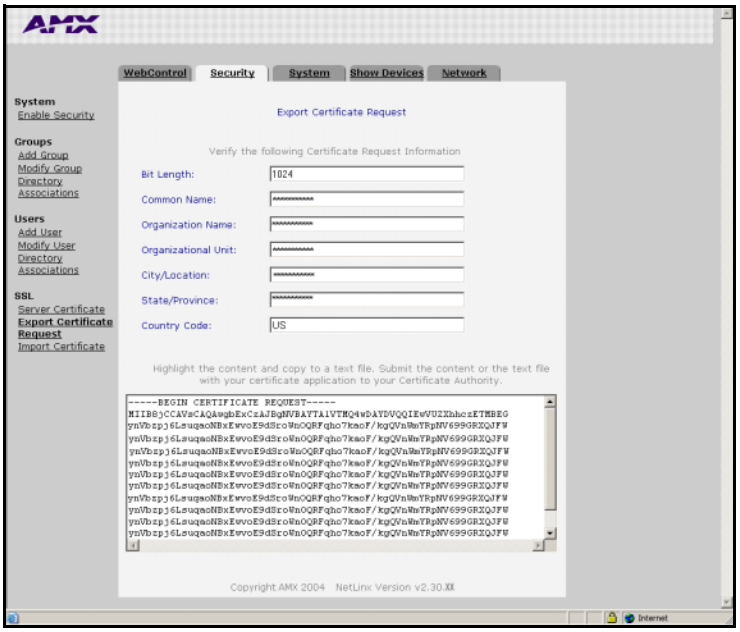


FIG. 34 Security Tab - Export Certificate Request field

Security tab - Import Certificate page

The **SSL > Import Certificate** link opens an Import Certificate field (FIG. 35) where an authorized user can paste the raw text from a CA issued Certificate.

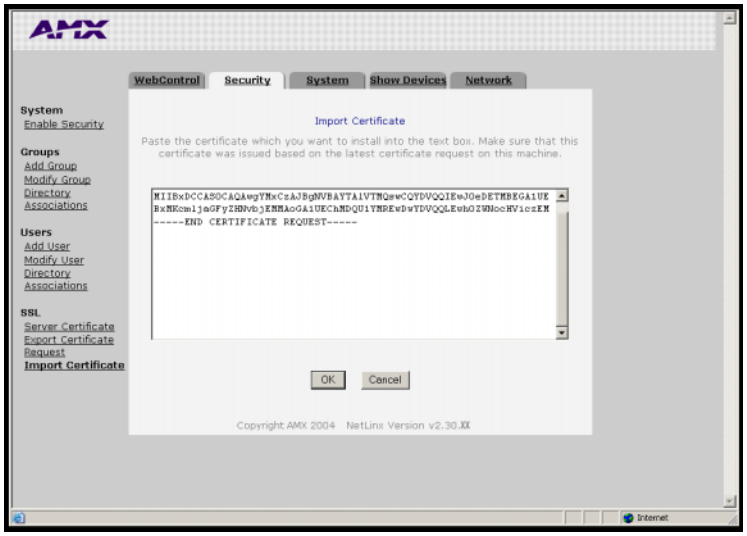


FIG. 35 Security Tab - Import Certificate field

CAUTION

A CA server certificate can only be imported to a target Master only after both a self-generated certificate has been created and the SSL Enable feature has been selected on the Master. These actions configure the Master the secure communication necessary during the importing of the CA certificate.

System Tab

Displays the firmware version and log information for the NetLinx Master (FIG. 36).

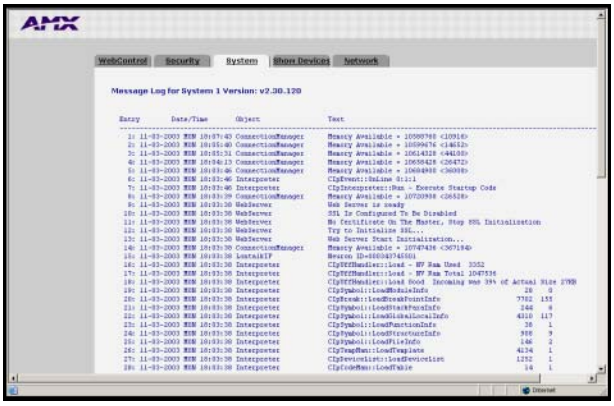


FIG. 36 System Tab

Show Devices Tab

Displays the device values and firmware versions of devices connected to the current NetLinx Master System (FIG. 37).

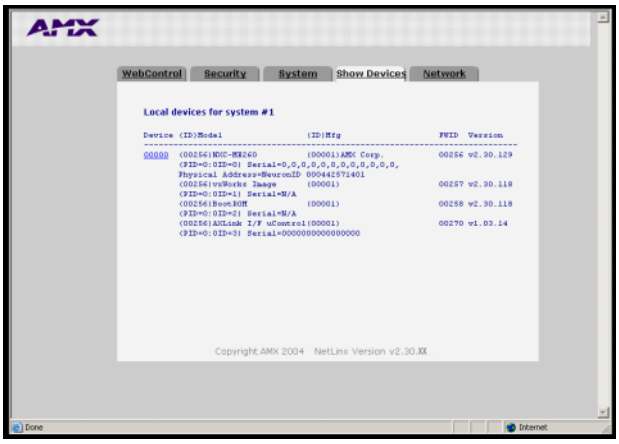


FIG. 37 Show Devices tab

Network Tab

Provides a list of the DNS and URL associated with the NetLinx Master.

- The DNS List identifies the Domain Name servers that translates domain names for the Master into IP Addresses.
- The URL List identifies all URL entries within the Master's URL list.

Master Security Setup Procedures

Setting the system security options for a NetLinx Master (Security Options Menu)

1. Enter the URL/IP Address of the target Master into the *Address/URL* field within the web browser. Refer to the *Accessing the NetLinx Master via an IP Address* section on page 35 for more detailed instructions on using your web browser to access your Master.
2. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window. Refer to the *Security Tab* section on page 37 for more detailed descriptions on the security configuration options.
3. Click the **Enable Security** link (on the left of the browser window) to populate the Security tab with NetLinx Master security options (FIG. 38) that can individually be enabled or disabled.

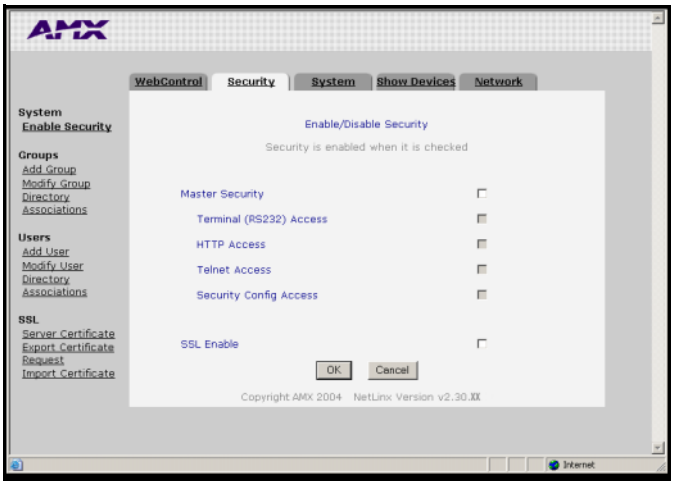


FIG. 38 Security tab - showing NetLinx Master security options

NOTE

By default, Master Security and SSL Enable are disabled (unchecked), including the Master Security subcomponents: Terminal Access, HTTP Access, Telnet Access, and Security Configuration Access.

4. Click on the checkbox next to **Master Security** to enable the security on the target Master. Placing a check in this field allows you to alter the security properties for the remaining Master Security options (Terminal/HTTP/Telnet/Security Configuration). Refer to the *Security tab - Enable Security page* section on page 38 for more detailed field descriptions.

NOTE

*Each selection simply toggles the security setting from enabled to disabled. Click **OK** after making any changes to these features so that those alterations are then saved to the target Master.*

5. Before enabling the SSL security, a user must first develop and then install a self-generated Certificate onto the Master. Refer to the *Self-Generating a SSL Server Certificate Request* section on page 62.

CAUTION

This initial installation allows users to then later install the different types of certificates (requested, self-generated, or regenerated).

6. Click on the checkbox next to **SSL Enable** to enable the use of SSL encryption and server certificate usage. Activating this feature requires the creation of a server certificate. Refer to the *SSL Certificate Procedures* section on page 61 for instructions on creating and requesting a server certificate for the target Master.

CAUTION

***Before initially enabling the SSL feature on the Master**, a self-generated certificate should first be installed. This initial certificate, along with the enabling of the SSL security feature (from the Enable Security page), allows users to create a secure connection to the Master so an encrypted CA server certificate can then be safely imported.*

7. Click **OK** to accept and save the changes made on this tab to the Master. Clicking **Cancel** voids any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab.

NOTE

*If a SSL certificate has been previously placed on the target Master, after clicking OK, a server certificate security alert might appear to inform you of any issues with the existing certificate. Click **Yes** to accept the certificate conditions and continue accessing the target Master.*

8. Successful incorporation of the changes to the Master's security configurations results in an on-screen message "System Security successfully configured. SSL has been turned on".

NOTE

A Group represents a logical collection of individual users. Any properties possessed by a group (ex: access rights, directory associations, etc.) are inherited by all members of that group.
The "administrator" group account cannot be deleted or modified.

Adding a Group and assigning their access rights

1. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window. Refer to the *Security tab - Add Group page* section on page 39 for more detailed descriptions on the security configuration options.
2. Click the **Add Group** link to populate the Security tab with the fields necessary for configuring a new group and assigning its associated access rights (FIG. 39).

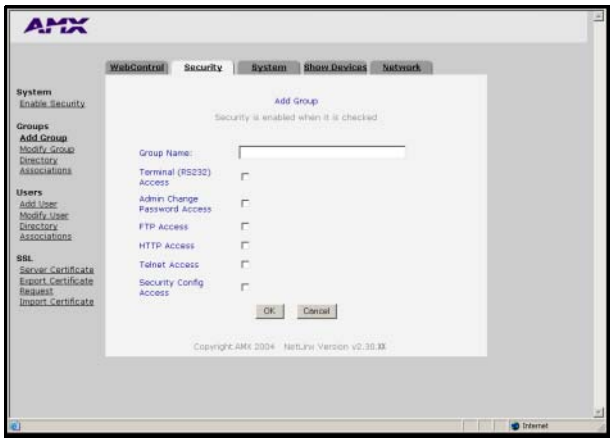


FIG. 39 Security tab - showing the Add Group fields

3. Enter a unique alpha-numeric string (consisting of 4 - 20 characters) into the Group Name field. This string provides a unique name for the desired group. **The word *administrator* cannot be used for a new group name since it already exists by default.**

4. Click on the checkbox next to the requested access rights desired for the selected group. Placing a check in these fields activates the access rights (Terminal/Admin Change/FTP/HTTP/Telnet/Security Configuration). Refer to the *Security tab - Add Group page* section on page 39 for more detailed field descriptions.
5. Click **OK** to accept and save the changes made on this tab to the Master. Clicking **Cancel** voids any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab.
6. Successful addition of the new group results in an on-screen message "Group 'XXX' added".

NOTE

Any security changes made to the Master from within the web browser are instantly reflected within a Terminal session without the need to reboot.
Security changes made to the Master from within a Terminal window are not reflected within the web browser until the Master is rebooted and the web browser connection is refreshed.

Modifying an existing Group's access rights

1. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window. Refer to the *Security tab - Modify Group page* section on page 40 for more detailed descriptions on the security configuration options.
2. Click the **Modify Group** link (on the left of the browser window) to populate the Security tab with the access rights fields associated with the selected group. (FIG. 40).

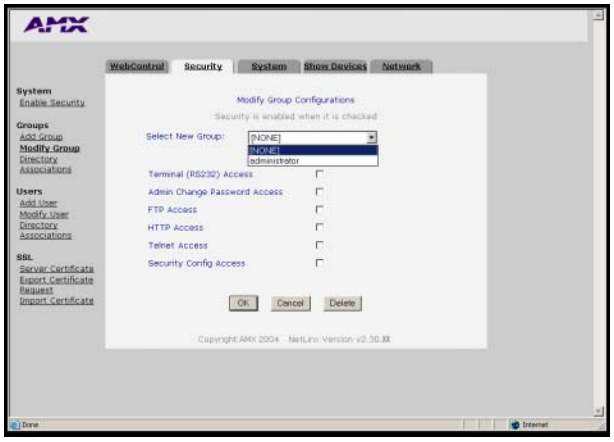


FIG. 40 Security tab - showing the Modify Group access rights fields

3. Click the down arrow from the *Select New Group* field to open a drop-down listing of **authorized groups**. Initially, *administrator* is listed as the last accessed group. As more groups are added through the Add Group section of the Security tab; those groups appear within the drop-down selection (along with checkmarks alongside their pre-configured access rights).
   - After a group is selected, the access rights, previously assigned to that group, are selected/enabled with a checkmark next the corresponding field (Terminal/Admin Change/FTP/HTTP/Telnet/Security Configuration). Refer to the *Security tab - Modify Group page* section on page 40 for more detailed field descriptions.
4. Enable (check) or disable (uncheck) the checkbox associated to the desired access right. Alterations made within this window modify any previously access rights that were assigned to the selected group when it was created.

5. Click **OK** to accept and save the changes made on this tab to the Master.

NOTE

*Clicking **Delete** removes the selected group from the list of authorized groups on the Master.*
*Clicking **Cancel** voids any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab.*

6. Successful modification of the new group results in an on-screen message "Group 'XXX' modified".

NOTE

Each selection simply toggles the security setting from enabled to disabled.

Showing a list of authorized Groups

1. Click on the **Security** tab (FIG. 40).
2. Click the **Modify Group** link (on the left of the browser window) to populate the Security tab with the access rights fields associated with a selected group.
3. Click the down arrow from the *Select New Grou*p field to open a drop-down listing of authorized groups on the target Master.

Deleting an existing Group

1. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window.
2. Click the **Modify Group** link.
3. Click the down arrow from the *Select New Group* field to open a drop-down listing of available groups.
4. Select a group from the drop-down listing.
5. Click **Delete** to remove the selected group from the list of authorized groups on the Master.
6. Successful deletion of the group results in an on-screen message "Group 'XXX' deleted".

Adding a Group directory association

1. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window. Refer to the *Security tab - Group Directory Associations page* section on page 41 for more detailed descriptions on the security configuration options.
2. Click the **Directory Associations** link (on the left of the browser window) to populate the Security tab with the directory associations assigned to the selected group (FIG. 41).

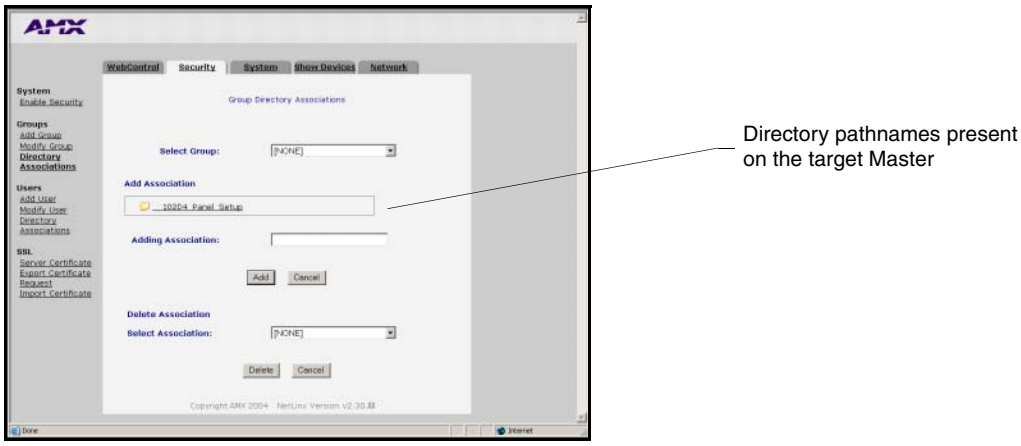


FIG. 41 Security tab - showing the Group Directory Associations fields

3. Click the down arrow from the *Select Group* field to open a drop-down listing of **authorized groups**. Initially, administrator is listed as a default group.
   - The Add Association field displays the current directory folders that currently reside within the target Master. These can consist of G3 HTML project folders, data file folders, etc.
4. Enter a new directory association path into the *Adding Association* field. This character string can range from 1 - 128 alpha-numeric characters. This string is case sensitive. This information is the path to the file or directory to which you want to grant access. A single '/' is sufficient to grant access to all files and directories in the user directory and it's subdirectory. The '/*' wildcard can also be added to enable access to all files. All entries should start with a '/'. Here are some examples of valid entries:

Valid Directory Association Entries

Path	Description
`/`	Enables access to the user directory and all files and subdirectories in that user directory.
`/*`	Enables access to the user directory and all files and subdirectories in that user directory.
`/user1`	If `user1` is a file in the user directory, only the file is granted access. If `user1` is a subdirectory of the user directory, all files in the `user1` and its sub-directories are granted access.
`/user1/`	`user1` is a subdirectory of the user directory. All files in the `user1` and its sub-directories are granted access.
`/Room1/iWebControlPages/*`	`/Room1/iWebControlPages` is a subdirectory and all files and its subdirectories are granted access.

*Not only can an **administrator** provide group access to a file or folder on the Master, but also to an Application tab displayed within the web browser (such as Show Devices or Network).*

- To add an association to an Application tab, enter the association location (ex: /showdevices.asp) into the *Adding Association* field.

5. Click **Add** to add the new directory path to the group and save it to the Master.
6. Successful modification of the new path results in an on-screen message, for example: "Directory Assocation '/XXX' added for group "XXX".
7. Click the down arrow from the *Select Association* field to open a drop-down listing of the associations for the selected group and confirm the added association appears in the list**.**

Confirming the new directory association

1. Click on the **Security** tab.
2. Click the **Directory Associations** link.
3. From the Delete Association section of the Group Directory Associations window, click the down arrow from the *Select Association* field to open a list of associations and confirm the new directory association has been assigned to the group.

Deleting a directory association

1. Click on the **Security** tab.
2. Click the **Directory Associations** link.
3. From the Delete Association section of the Group Directory Associations window, click the down arrow from the *Select Association* field to open a list of associations.
4. Select a directory association from the drop-down list.
5. Click **Delete** to remove the selected directory path from the group properties and save the change to the Master.
6. Successful deletion of the path results in an on-screen message, for example: "Directory Assocation '/XX' deleted for group "XXX".

A User represents a single potential client of the NetLinx Master. Any properties possessed by a group (ex: access rights, directory associations, etc.) are inherited by all users who are assigned to that group.
The "administrator" user account cannot be deleted or modified.

Adding a User and configuring their access rights

1. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window. Refer to the *Security tab - Add User page* section on page 43 for more detailed descriptions on the security configuration options.
2. Click the **Add User** link (on the left of the browser window) to populate the Security tab with the fields necessary for configuring a new user and assigning its associated access rights (FIG. 42).

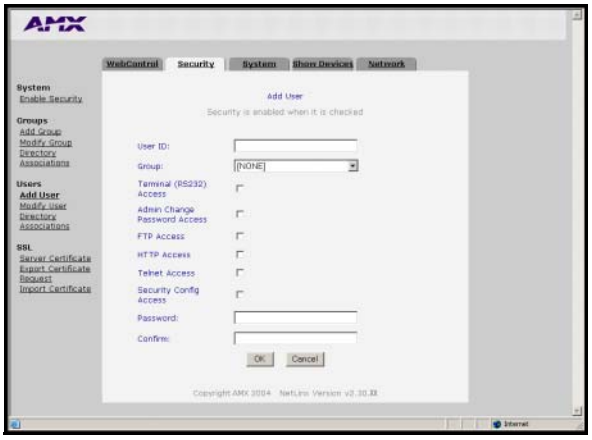


FIG. 42 Security tab - showing the Add User fields

3. Enter a unique alpha-numeric string (consisting of 4 - 20 characters) into the User ID field. This string provides a unique name for the desired user. **The user names *administrator* and *NetLinx* cannot be used since they already exist.**
4. Click the down arrow from the *Group* field to open a drop-down listing of **authorized groups**.
5. Click on the checkbox next to the requested access rights desired for the selected user. Placing a check in these fields activates the access rights (Terminal/Admin Password Change/FTP/HTTP/Telnet/Security Configuration). Refer to the *Security tab - Add User page* section on page 43 for more detailed field descriptions.

NOTE

*The **NetLinx** account can be deleted from either the Modify Group or User pages. The **administrator** account **can not be deleted** from either Modify pages and can not have it's directory associations modified.*

6. Enter the same password for the new user into both the *Password* and *Confirm* fields.
   - A user password is a valid character string (4 - 20 alpha-numeric characters) that is used to supplement the user name/ID in defining the potential client. The string is case sensitive and must be unique.
7. Click **OK** to accept and save the changes made on this tab to the Master. Pressing **Cancel** voids any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab.
8. Successful addition of the new group results in an on-screen message "User 'XXXX' was successfully added".

NOTE

Each selection simply toggles the security setting from enabled to disabled.

Modifying an existing User's access rights

1. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window. Refer to the *Security tab - Modify User page* section on page 44 for more detailed descriptions on the security configuration options.
2. Click the **Modify User** link (on the left of the browser window) to populate the Security tab with the access rights fields associated with the selected group. (FIG. 43).

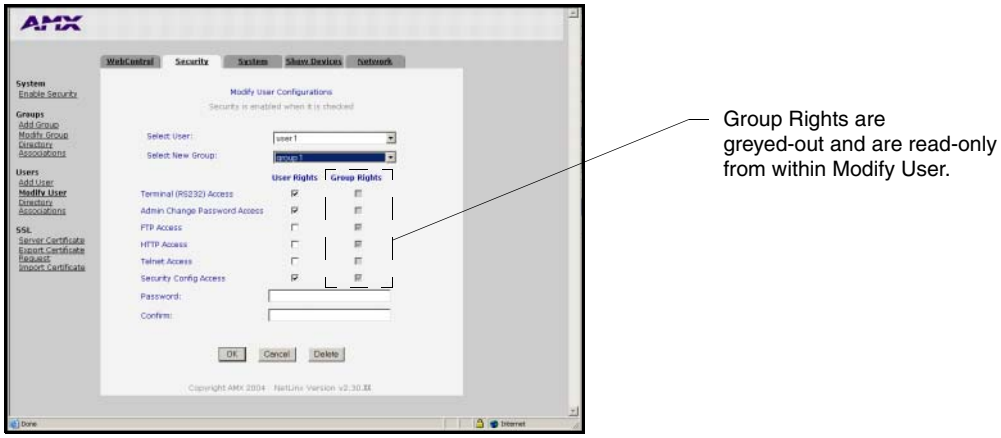


FIG. 43 Security tab - showing the Modify User Configurations fields

3. Click the down arrow from the *Select User* field to open a drop-down listing of **authorized users**. Initially, administrator and NetLinx are listed as default users. As more users are added through the Add User section of the Security tab; those users appear within the drop-down selection (along with checkmarks alongside their pre-configured access rights).
   - After a user is selected, the access rights, previously assigned to that user during creation, are selected/enabled with a checkmark next the corresponding field (Terminal/Admin Change/FTP/HTTP/Telnet/Security Configuration). Refer to the *Security tab - Modify User page* section on page 44 for more detailed field descriptions.
4. Click the down arrow from the *Select New Group* field to open a drop-down listing of **authorized groups** and assign the user to that group. Initially, administrator is listed as a default group. As more groups are added through the Add Group section of the Security tab; those groups appear within the drop-down selection (along with checkmarks alongside their pre-configured access rights).

NOTE

Any previously configured user access rights are populated in the left checkbox column. A previously created group's access rights are populated in the right checkbox column. Any properties possessed by a group (ex: access rights, directory associations, etc.) are inherited by all users who are assigned to that group.

5. Enable (check) or disable (uncheck) the checkboxes associated to the desired user access rights. Alterations made within this window modify any previously access rights that were assigned to the selected user when it was created.

6. Enter the same password for the user into both the *Password* and *Confirm* fields, if you want to change the password. *Leaving this field blank retains the current or previous password.*
   - A user password is a valid character string (4 - 20 alpha-numeric characters) that is used to supplement the user name/ID in defining the potential client. The string is case sensitive and must be unique.
7. Click **OK** to accept and save the changes made on this tab to the Master.

NOTE

*Clicking **Cancel** voids any changes made within this tab, disables the security configuration session, voids any changes made to the Master, and returns you to the empty Security tab.*
*Clicking **Delete** removes the selected user from the list of authorized users on the Master.*

8. Successful modification of the new user results in an on-screen message "User 'XXX' modified".

NOTE

Each selection simply toggles the security setting from enabled to disabled.

Showing a list of authorized Users

1. Click on the **Security** tab.
2. Click the **Modify User** link (on the left of the browser window) to populate the Security tab with the access rights fields associated with the selected user.
3. Click the down arrow from the *Select User* field to open a drop-down listing of authorized users on the target Master.

Deleting a User

1. Click on the **Security** tab (FIG. 43 on page 58). By default this tab is blank until a security option is selected from the left of the browser window.
2. Click the **Modify User** link (on the left of the browser window) to populate the Security tab with the access rights fields associated with the selected user.
3. Click the down arrow from the *Select User* field to open a drop-down listing of authorized users on the target Master.
4. Select a user from the drop-down listing.
5. Click **Delete** to remove the selected user from the list of authorized users on the Master.
6. Successful deletion of the user results in an on-screen message "User 'XXX' deleted".

Adding a User directory association

1. Click on the **Security** tab. By default this tab is blank until a security option is selected from the left of the browser window. Refer to the *Security tab - User Directory Associations page* section on page 45 for more detailed descriptions on the security configuration options.
2. Click the **Directory Associations** link (on the left of the browser window) to populate the Security tab with the directory associations assigned to the selected user (FIG. 44).

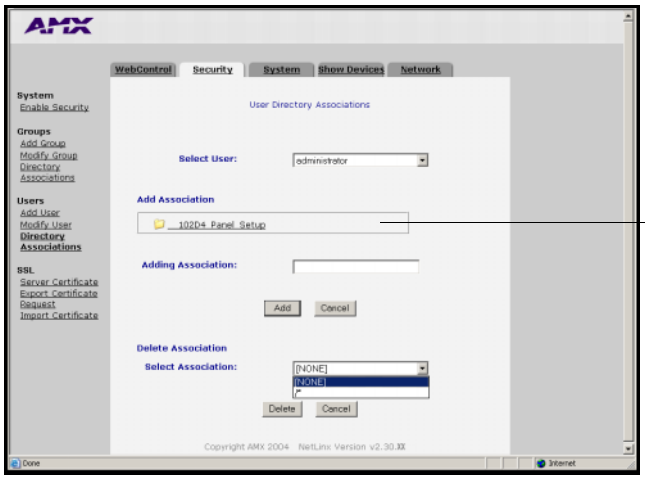


FIG. 44 Security tab - showing the User Directory Associations fields

3. Click the down arrow from the *Select User* field to open a drop-down listing of **authorized users**. Initially, administrator and NetLinx are listed as default users.
   - The Add Association field displays the current directory folders that currently reside within the target Master. These can consist of G3 HTML project folders, data file folders, etc.
4. Enter a new directory association path into the *Adding Association* field. This character string can range from 1 - 128 alpha-numeric characters. This string is case sensitive. This information is the path to the file or directory to which you want to grant access. A single '/' is sufficient to grant access to all files and directories in the user directory and it's subdirectory. The '/*' wildcard can also be added to enable access to all files. All entries should start with a '/'.

NOTE

*Not only can an **administrator** provide user access to a file or folder on the Master, but also to an Application tab displayed within the web browser (such as Show Devices or Network).*

   - To add an association to an Application tab, enter the association location (ex: /showdevices.asp) into the *Adding Association* field.
5. Click **Add** to incorporate the new directory path to the user and save it to the Master.
6. Successful modification of the new path results in an on-screen message, for example: "Directory Assocation '/XXX' added for user "XXX".
7. Click the down arrow from the *Select Association* field to open a drop-down listing of the associations for the selected group and confirm the added association appears in the list.

Confirming the new directory association

1. Click on the **Security** tab.
2. Click the **Directory Associations** link.
3. From the Delete Association section of the User Directory Associations window, click the down arrow from the *Select Association* field to open a list of associations and confirm the new directory association has been assigned to the user.

Deleting a directory association

1. Click on the **Security** tab.
2. Click the **Directory Associations** link.
3. From the Delete Association section of the User Directory Associations window, click the down arrow from the *Select Association* field to open a list of associations.
4. Select a directory association from the drop-down list.
5. Click **Delete** to remove the selected directory path from the user properties and save the change to the Master.
6. Successful deletion of the path results in an on-screen message, for example: "Directory Assocation '/XXX' deleted for user "XXX".

SSL Certificate Procedures

Initially, a NetLinx Master is not equipped with any installed certificates. **In order to prepare a Master for later use with CA** (*officially issued*) **server certificates**, it is necessary to:

- **First create a self-generated certificate** which is automatically installed onto the Master.
- Secondly, enable the SSL feature from the Enable Security page. Enabling SSL security after the certificate has been self-generated insures that the target Master is utilizing a secure connection during the process of importing a CA server certificate over the web.

A self-generated certificate has lower security than an external CA generated certificate.

Self-Generating a SSL Server Certificate Request

1. Click on the **Security** tab (FIG. 45). Refer to the *Security tab - SSL Server Certificate page* section on page 47 for more detailed descriptions on the security configuration options.
2. Click the **Server Certificate** link (on the left of the browser window) to display the Security tab with the fields necessary for developing a new certificate.

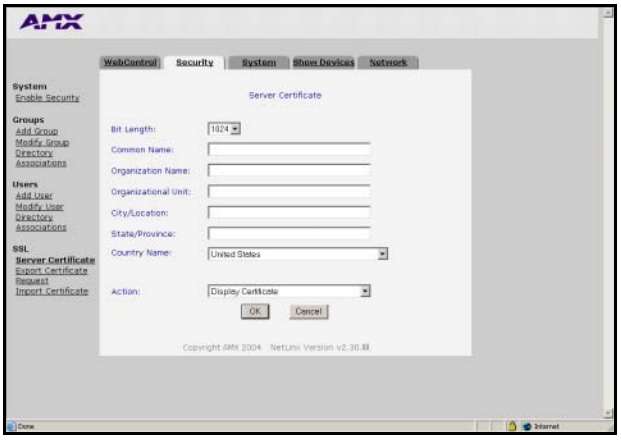


FIG. 45 Security tab - showing the Server Certificate creation fields

3. Click the down arrow from the *Bit length* field to open a drop-down listing of available public key lengths.
   - The three available public key lengths are: 512, 1024, and 2048. Higher selected key lengths result is increased certificate processing times. A larger the key length results in more secure certificates.
4. Enter the Domain Name.
   - Example: If the address being used is www.amxuser.com, that must be the Common name and format used in the *Common Name* field. This string provides a unique name for the desired user.
   - **This domain name does not need to be resolvable URL Address when self-generating a certificate.**
5. Enter the name of the business or organization into the *Organization Name* field. This is an alpha-numeric string (1 - 50 characters in length).
6. Enter the name of the department using the certificate into the *Organizational Unit* field. This is an alpha-numeric string (1 - 50 characters in length).
7. Enter the name of the city where the certificate will reside into the *City/Location* field. This is an alpha-numeric string (1 - 50 characters in length).
8. Enter the name of the state or province where the certificate will reside into the *State/Province* field. This is an alpha-numeric string (1 - 50 characters in length).
   The city/province name must be fully spelled out.
9. Click the down arrow from the *Country Name* field to open a drop-down listing of listing of currently selectable countries.
10. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.

11. Choose **Self Generate Certificate** from the drop-down list. *When this request is submitted, the certificate is generated and installed into the Master in one step.*
12. Click **OK** to save the new encrypted certificate information to the Master or click **Cancel** to void any changes made within this tab and exit without making changes to the target Master.

ONLY use the Regenerate certificate option when you have Self Generated your own certificate. DO NOT regenerate an external CA-generated certificate.

13. Click the **Security** tab > **Enable Security** link to return to the Enable Security page.
14. Place a checkmark into the SSL Enable selection box to enable the SSL security feature on the target Master. **Activating this option creates a secure connection to and from the target Master. It is recommended that a secure connection to the target Master be used when importing a CA server certificate.**

Creating a Request for a SSL Server Certificate

1. Click on the **Security** tab. Refer to the *Security tab - SSL Server Certificate page* section on page 47 for more detailed descriptions on the security configuration options.
2. Click the **Server Certificate** link (on the left of the browser window) to display the Security tab with the fields necessary for generating a new certificate.
3. Click the down arrow from the *Bit length* field to open a drop-down listing of available public key lengths.
   - The three available public key lengths are: 512, 1024, and 2048. Higher selected key lengths result in increased certificate processing times. A longer key length results in more secure certificates.
4. Enter the used Domain Name.
   - Example: If the address being used is www.amxuser.com, that must be the Common name and format used in the *Common Name* field. This string provides a unique name for the desired user.
   - **This domain name must be associated to a resolvable URL Address when creating a request for a purchased certificate. The address does not need to be resolvable when obtaining a free certificate.**
5. Enter the name of the business or organization into the *Organization Name* field. This is an alpha-numeric string (1 - 50 characters in length).
6. Enter the name of the department using the certificate into the *Organizational Unit* field. This is an alpha-numeric string (1 - 50 characters in length).
7. Enter the name of the city where the certificate will reside into the *City/Location* field. This is an alpha-numeric string (1 - 50 characters in length).
8. Enter the name of the state or province where the certificate will reside into the *State/Province* field. This is an alpha-numeric string (1 - 50 characters in length).
   The state/province name must be fully spelled out.
9. Click the down arrow from the *Country Name* field to open a drop-down listing of listing of currently selectable countries.

10. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.
11. Choose **Create Request** from the drop-down list.
12. Click **OK** to accept the information entered into the above fields and generate a certificate file. Refer to the *Security tab - Export Certificate Request page* section on page 49.
    - This refreshed the Server Certificate page and if the certificate request was successful, displays a "Certified request generated" message.
13. Click the **Export Certificate Request** link (on the left of the browser window) to display the certificate text file.
14. Place your cursor within the certificate text field.
15. Press the **Ctrl** + **A** keys simultaneously on your keyboard (this selects all the text within the field).

YOU MUST COPY ALL OF THE TEXT *within this field, including the* ***-----BEGIN CERTIFICATE REQUEST-----*** *and the* ***-----END CERTIFICATE REQUEST-----.*** *Without this text included in the CA submission, you will not receive a CA-approved certificate.*

16. Press the **Ctrl** + **C** keys simultaneously on your keyboard (this takes the blue selected text within the field and copies it to your temporary memory/clipboard).
17. Paste this text into your e-mail document and then send that information to a CA with its accompanying certificate application.

When a certificate request is generated, you are creating a private key on the Master. ***YOU CAN NOT REQUEST ANOTHER CERTIFICATE UNTIL THE PREVIOUS REQUEST HAS BEEN FULFILLED.*** *Doing so will void any information received from the previously requested certificate and it will be nonfunctional if you try to use it.*

18. Once you have received the returned CA certificate, follow the procedures outlined in the following section to import the returned certificate, over a secure connection, to the target Master.

Importing a CA certificate to the Master over a secure SSL connection

Before importing a CA server certificate, you must:

- **First**, have a self-generated certificate installed onto your target Master.
- **Secondly**, enable the SSL security feature from the Enable Security page, to establish a secure connection to the Master prior to importing the encrypted CA certificate. Refer to the *Security tab - Enable Security page* section on page 38 for more information about enabling SSL security.

1. Take the returned certificate (signed by the CA and encrypted with new information which makes it different from the text string that was previously sent) and copy it into your clipboard. Refer to the *Security tab - Import Certificate page* section on page 49.
2. Click the **Import Certificate** link to open the empty Import Certificate window.
3. Place your cursor within the empty window and paste the raw text data (in its entirety) into the field.

4. Click **OK** to enter the new encrypted certificate information and save it to the Master or click **Cancel** to void any changes made within this tab and exit without making changes to the target Master.

CAUTION

*Once a certificate has been purchased from an external CA and then installed onto a specific Master, **DO NOT regenerate the certificate or alter its properties** (example: bit length, city, etc.).If the purchased certificate is regenerated, it becomes invalid.*

A certificate consists of two different Keys:

- **Master Key** is generated by the Master and is incorporated into the text string sent to the CA during a certificate request. It is specific to a particular request made on a specific Master.
- **Public Key** is part of the text string that is returned from the CA as part of an approved SSL Server Certificate. This public key is based off the submitted Master key from the original request.
- **Regenerating a previously requested and installed certificate, invalidates the previously purchased certificate because the Master Key has been changed.**

5. Use the *Display Certificate* option to confirm that the new certificate was imported properly to the target Master.

Display SSL Server Certificate Information

1. Click on the **Security** tab (FIG. 45 on page 62). Refer to the *Security tab - SSL Server Certificate page* section on page 47 for more detailed descriptions on the security configuration options.
2. Click the **Server Certificate** link (on the left of the browser window) to populate the Security tab.

NOTE

By default, the Display Certificate Action is selected and these fields are populated with information from an installed certificate. If the Master does not have a previously installed certificate, these fields are blank.

3. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.
4. Choose **Display Certificate** from the drop-down list.
5. Click **OK** to accept the action and populate the fields with the certificate information.

Regenerating an SSL Server Certificate Request

1. Click on the **Security** tab. Refer to the *Security tab - SSL Server Certificate page* section on page 47 for more detailed descriptions on the security configuration options.
2. Click the **Server Certificate** link (on the left of the browser window) to display the Security tab with the fields necessary for developing a new certificate.

This method of certificate generation is used to modify or recreate a previously existing certificate already on the Master.
By default, if a certificate is already present on the target Master, the Display Certificate Action is selected and these fields are populated with information.
EX: if the company has moved from Dallas to Houston, all of the information is reentered exactly except for the City.

3. Enter any new or changed information into its respective field.
4. Click the down arrow from the *Action* field to open a drop-down listing of available certificate generation options.
5. Choose **Regenerate Certificate** from the drop-down list.

When this request is submitted, the certificate is generated and installed into the Master in one step.

6. Click **OK** to save the newly modified certificate information to the Master or click **Cancel** to void any changes made within this tab and exit without making changes to the target Master.
7. **Before exiting the Master and beginning another session**:
   - verify that all users have been assigned the correct rights, and are using the correct passwords.
   - In the Enable Security window of the Security tab, verify that the Master Security and HTTP Access are enabled. Enabling HTTP Access will prompt users to enter pre-configured user names and passwords.

Common Steps for Requesting a Certificate from a CA

A certificate is a cryptographically signed object that associates a public key and an identity. Certificates also include other information in extensions such as permissions and comments. A "**CA**" is short for Certification Authority and is an internal entity or trusted third party that issues, signs, revokes, and manages these digital certificates.

1. Navigate to the Web Server Certificate HTML page on your CA's website.
   - A Web Server certificate allows you to authenticate through a Web browser via SSL. In order to successfully verify other certificates it is also necessary to import the CA key into the Web Server. Refer to the *Creating a Request for a SSL Server Certificate* section on page 63.
   - This is done as part of the process of receiving your Web Server certificate.
   - **Only a user with administrator privileges can request a server certificate.**
2. Enter in the company information, such as: name, e-mail, address, state, and country.
3. Agree to any licensing agreements and continue to the next part of the registration process.

4. Enter the name of the server being used (this is the Master).
   - The server name is the name as it shows up in the URL of the Master you are securing with this server certificate. For example, if the URL of the Master will be https://www.myNetLinxMaster.com/, then enter the server name as www.myNetLinx Master.com.
5. Send the CA the text created by your certificate request through the Master. Refer to the *Creating a Request for a SSL Server Certificate* section on page 63 for the procedures necessary to generate the certificate text file.
6. Place your cursor within the certificate text field of the Export Certificate window of the Security tab.
7. Press the **Ctrl + A** keys simultaneously on your keyboard (this selects all the text within the field).

YOU MUST COPY ALL OF THE TEXT *within this field, including the* ***-----BEGIN CERTIFICATE REQUEST-----*** *and the* ***-----END CERTIFICATE REQUEST-----.*** *Without this text included in the CA submission, you will not receive CA approved certificate.*

8. Press the **Ctrl + C** keys simultaneously on your keyboard (this takes the blue selected text within the field and copies it to your temporary memory/clipboard).
9. Paste this text into the *Submit Request* field on the CA's Retrieve Certificate web page.
10. Choose to view the certificate response in raw DER format.
11. Note the **Authorization Code** and **Reference Number** (for use in the e-mail submission of the request).
12. Submit the request.
13. Paste this certificate text field (copied from steps 7 & 8 above) into your e-mail document and then send that information to a CA with its accompanying certificate application.
14. Complete the certificate installation procedures outlined in the *Creating a Request for a SSL Server Certificate* section on page 63.

Accessing an SSL-Enabled Master via an IP Address

1. Enter the IP Address of the target Master (***example: 198.198.99.99***) into the web browser *Address* field.
2. Press the Enter key on your keyboard to begin the communication process between the target Master and your computer.
3. The user is then presented with a Security Alert popup window and Certificate information (FIG. 46).

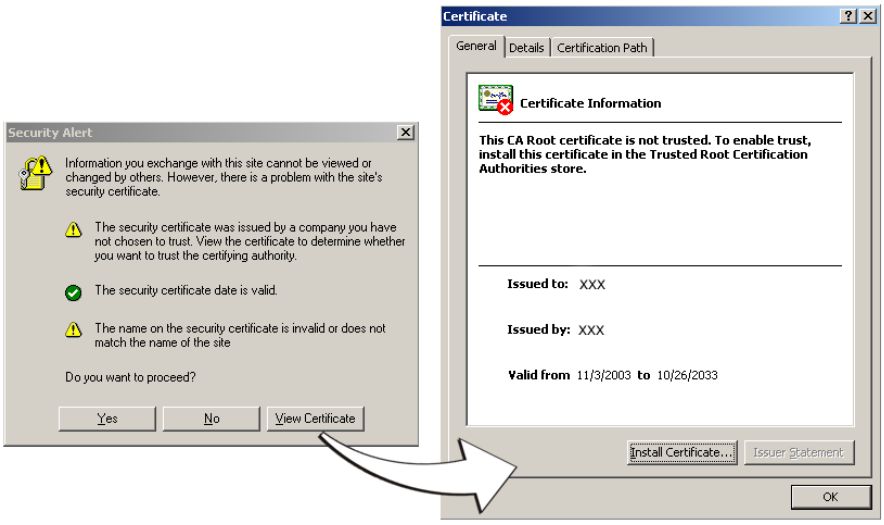


FIG. 46 Security Alert and Certificate popups

NOTE

The above alert will only appear if an SSL Server Certificate has been installed on the target Master, the SSL Enable options has been enabled, from within the Enable Security window of the Security tab, and there is a problem with the site's certificate.

Problems with the certificate can result from:

- A self generated and self-signed certificate that hasn't been approved by a CA.
- The self-generated certificate is not part of that computer's web browser list of trusted sites. This changes after the certificate is installed into the user's browser list of trusted sites.
- The date period given to the certificate has expired. CA-approved certificates typically come with a 2 year window of validity. Self generate certificates come defaulted with a 30 year window of validity (see FIG. 46).
- The name on the security certificate site information doesn't match the domain name of the target Master.

4. Click the **View Certificate** button on the Security Alert popup to view more detailed information about the certificate. A secondary Certificate popup window is then displayed.
5. Review the information presented within the certificate and if you trust that both the site and certificate information are correct, click the **Install Certificate** button to begin installing the certificate into computer's web browser list of trusted sites.

6. The user is then presented with a Certificate Import Wizard that begins the process of adding the certificate (FIG. 47).

FIG. 47 Certificate Import Wizard

7. Click **Next** to proceed with the certificate store process.

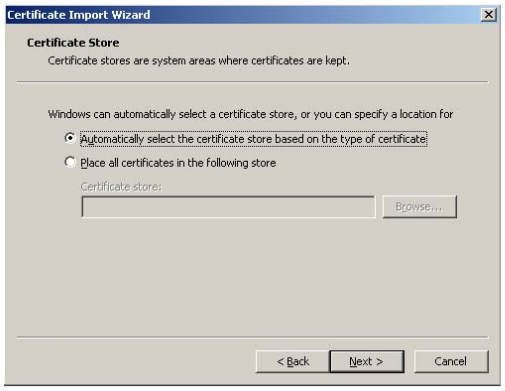


FIG. 48 Certificate Import Wizard- storing the certificate

8. Click **Next** to automatically use the default certificate store settings and locations (FIG. 48).
9. Click **Finish** button to finalize the certificate installation process.
10. Click **Yes**, from the next popup window to *"...ADD the following certificate to the Root Store?"*. After a successful importing of the certificate into Internet Explorer's list of trusted sites, another popup window appears to inform you of the success.
11. Click **OK** from the Import was successful popup window.
12. To close the still open Certificate popup window click **OK**.
13. To close the still open Security Alert popup window, click **Yes**.
14. From the Network Password window, click the down arrow from the *user name* field to select a user name.
15. Enter a valid password into the *password* field.
16. Click the *save password* check mark field if you want to have your web browser remember this password during consecutive login sessions.
17. Click **OK** to access the target Master.

18. The first tab displayed within your open browser window is WebControl.

Using your NetLinx Master to control the G4 panel

Refer to the specific panel instruction manual for detailed information on configuring and enabling WebControl.

Once the Master's IP Address has been set through NetLinx Studio (version 2.1 or higher):

1. Launch your web browser.

NOTE

In order to fully utilize the SSL encryption, your web browser should incorporate the an encryption feature. This encryption level is displayed as a Cipher strength.

2. Enter the IP Address of the target NetLinx Master (***example: 198.198.99.99***) into your web browser's *Address* field.

3. Enter a valid user name and password into the fields within the Enter Network Password dialog.

4. Click **OK** to enter the information and proceed to the Master's WebControl tab.

5. Press the **Enter** key on your keyboard to begin the communication process between the target Master and your PC.

NOTE

If a Security Alert window appears on your computer screen, refer to the specific NetLinx Master Instruction Manual for detailed information regarding this popup window. These steps are based on a Master with proper security and SSL encryption enabled.

6. This tab (FIG. 25) displays links to both G3 web panel pages downloaded to the target Master and G4 panels running the latest G4 Web Control feature. **G3 can't be controlled with firmware greater than 139. The ME260 cannot use firmware greater then 139.**

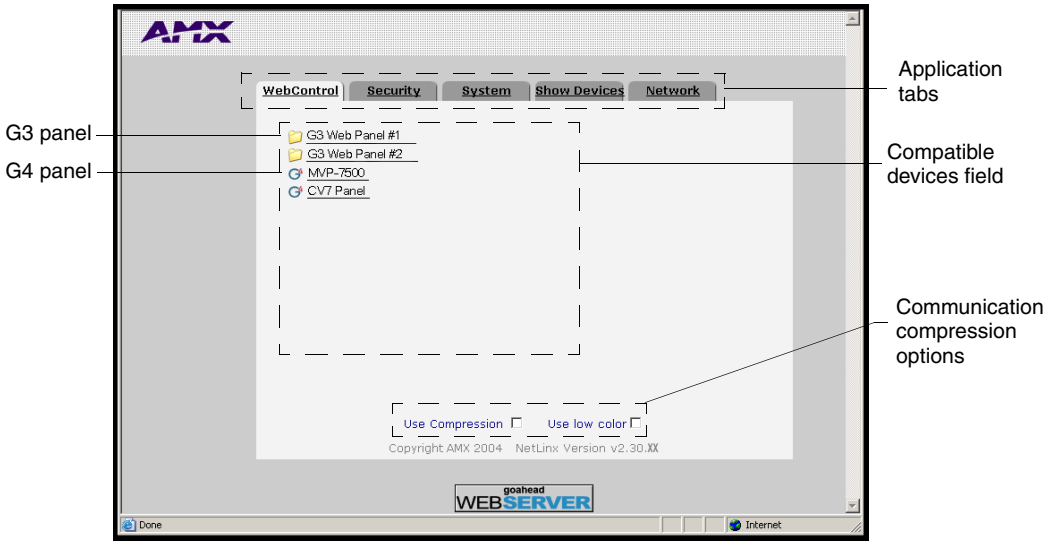


FIG. 49 WebControl Tab (populated with panels)

7. Click on the G4 panel name link associated with the target panel. A secondary web browser window appears on the screen (FIG. 50).

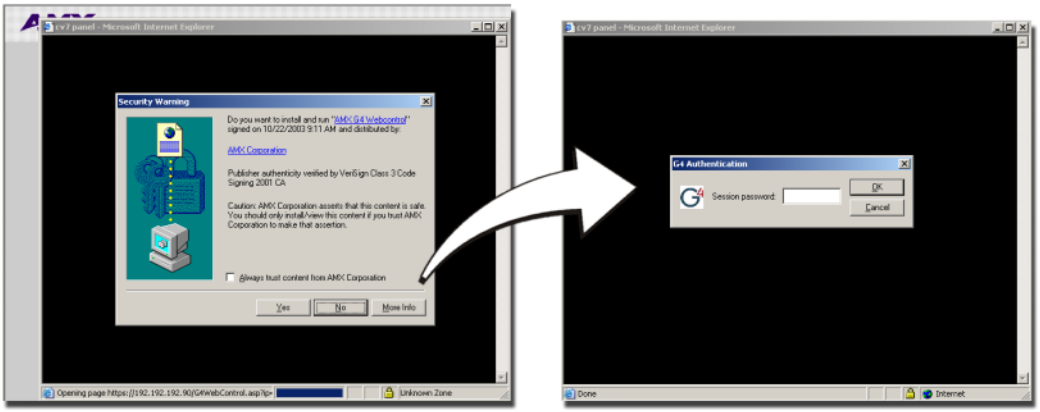


FIG. 50 WebControl VNC installation and Password entry screens

8. Click **Yes** from the Security Alert popup window to agree to the installation of the G4 WebControl application on your computer. This application contains the necessary Active X and VNC client applications necessary to properly view and control the panel pages from your computer.

NOTE

The G4 WebControl application is sent by the panel to the computer that is used for communication. Once the application is installed, this popup will no longer appear. This popup will only appear if you are connecting to the target panel using a different computer.

9. If a WebControl password was setup on the G4 WebControl page, a G4 Authentication Session password dialog box appears on the screen within the secondary browser window.
10. Enter the WebControl session password into the Session password field (FIG. 50).
11. Click **OK** to send the password to the panel and begin the session.

The secondary window then becomes populated with the same G4 page being displayed on the target G4 panel. A small circle appears on the G4 panel page and corresponds to the location of the mouse cursor. A left-mouse click on the computer-displayed panel page equates to an actual touch on the target G4 panel page.

Using your NetLinx Master to control the G3 panel

Refer to the specific panel instruction manual for detailed information on configuring and enabling WebControl. Before being able to access a G3 panel (with SSL enabled) through the WebControl tab, you must first download the Java Virtual Machine software from Sun Micro Systems® to install a Sun Java applet on your computer. **G3 can't be controlled with firmware greater than 139. The ME260 cannot use firmware greater then 139.**

NOTE

You must install the Sun Java Web Start application. ***Using the default Microsoft® Java applet (when SSL is enabled) can cause some G3 panels not to open or be viewed properly.***

Once the Master's IP Address has been set through NetLinx Studio (version 2.1 or higher):

1. Navigate to the Java Web Start Application from **http://java.sun.com/products**.

2. Click on the **Download Java Web Start > Download Java Web Start 1.4.2** link to begin the download of the application to your hard drive and follow the installation procedures recommended by the application.
3. Restart your computer and launch your browser.
4. Repeat steps 1 - 5 from the previous section to launch the WebControl tab associated with your Master.
5. Click on the **G3** panel name link associated with the target panel.
6. A secondary web browser window appears on the screen to notify you that the computer is ***Loading the Java Virtual Machine***.

What to do when a Certificate Expires

Self-generated certificates have a duration period of approximately 30 years. Most externally requested CA certificates are generally valid for a period of approximately 1 - 5 years.

The only way to avoid a CA certificate becoming invalid due to a time expiration is to request a new certificate from your current CA.

Refer to the *Creating a Request for a SSL Server Certificate* section on page 63 for more information on how to request an externally generated certificate.

NetLinx Security with a Terminal Connection

NetLinx ME260 Masters (**build 139**) have built-in security capabilities. It will require a valid user name and password to access the NetLinx System's Telnet, HTTP and FTP servers.

The security capabilities are configured and applied via a Telnet connection or the NetLinx Master's RS-232 terminal interface (the RS232 Program port).

NOTE

Always use the RS232 Program port when entering potentially sensitive security information. The Telnet server interface exposes this security information to the network in clear text format, which could be intercepted by an unauthorized network client. By using the RS232 Program port, there is security during the configuration of the database due to the physical proximity of the user to the system.

NetLinx Security Features

NetLinx security allows you to define access rights for users or groups.

NOTE

A "User" represents a single potential client of the NetLinx Master, while a "Group" represents a logical collection of users. Any properties possessed by groups (i.e., access rights, directory associations, etc.) are inherited by all the members of the group.

The following table lists the NetLinx features that the administrator (or other 'qualified' user) may grant or deny access to.

NetLinx Security Features	
NetLinx Master Security Configuration	The user has access to the security configuration commands of the Master. Only those users with security configuration access rights granted will have access to the security configuration commands.
Telnet Security	The user has access to the Telnet server functionality. All basic commands are available to the user.
Terminal (RS232 Program port) Security	The user has access to the Terminal (RS232 Program port) server functionality. All basic commands are available to the user.
HTTP (web server) Security	The user has access to the HTTP server functionality. Directory associations assign specific directories/files to a particular user.
FTP Security	The user has access to the FTP server functionality. Only the administrator account has access to the root directory; all other 'qualified' clients are restricted to the /user/ directory and its 'tree'.

Initial Setup via a Terminal Connection

Security administration and configuration is done via a Terminal communication through the RS232 Program port on the NetLinx Master.

Establishing a Terminal connection

1. Launch the HyperTerminal application from its' default location (**Start > Programs > Accessories > Communications**).
2. Apply power to the NetLinx Master and allow it to boot up.
3. Connect the PC COM (RS232) port to the RS232 Program port on the NetLinx Master. *Note the baud rate settings for the Master.*

4. Enter any text into the *Name* field of the HyperTerminal Connection Description dialog window and click **OK** when done.
5. From the *Connect Using* field, click the down-arrow and select the COM port being used for communication by the target Master.
6. Click **OK** when done.
7. From the *Bits per second* field, click the down-arrow and select the baud rate being used by the target Master.
   - Configure the remaining communication parameters as follows: Data Bits:8, Parity:None, Stop bits:1, and **Flow control: None** *(default is Hardware)*.
   - Click **OK** to complete the communication parameters and open a new Terminal window.
8. Type **echo on** to view the characters while entering commands.

Accessing the Security configuration options

1. In the Terminal session, type **help security** to view the available security commands. Here is a listing of the security help:

```
---- These commands apply to the Security Manager and Database ----
logout                  Logout and close secure session
setup security          Access the security setup menus
```

2. Type **setup security** to access the Main Security Menu, shown below:

```
>setup security

--- These commands apply to the Security Manager and Database ----
 1) Set system security options for NetLinx Master
 2) Display system security options for NetLinx Master
 3) Add user
 4) Edit user
 5) Delete user
 6) Show the list of authorized users
 7) Add group
 8) Edit group
 9) Delete group
10) Show list of authorized groups
11) Set Telnet Timeout in seconds
12) Display Telnet Timeout in seconds
13) Make changes permanent by saving to flash


Or <ENTER> to return to previous menu

Security Setup ->
```

3. The Main Security Menu shows a list of choices and a prompt. To select one of the listed choices, simply enter the number of the choice (1-13) at the prompt and press <ENTER>.
4. Each option in the Main Security Menu displays a sub-menu specific to that option.

The following sub-section describe using each of the Main Security Menu options.

For a detailed description of each option in the Main Security Menu, refer to *Main Security Menu on page 84*.

Option 1 - Set system security options for NetLinx Master (Security Options Menu)

Type **1** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to display the **Security Options Menu**.

The Security Options Menu sets the "global" options for the NetLinx Master. It is accessed by the Set Security system options of the Main Security Menu. This first thing that will happen is you will be asked one of two questions. If NetLinx Master security is enabled, you will see the following:

```
NetLinx Master security is Enabled
Do you want to keep NetLinx Master security enabled? (y or n):
```

- If you answer **y** for yes, security will remain enabled and you will be taken to the Security Options Menu.
- If you answer **n** for no, all security settings (except FTP security) will be disabled and you will be taken back to the Main Security Menu.

If NetLinx Master security is not enabled, you will see the following:

```
NetLinx Master security is Disabled
Do you want to enable security for the NetLinx Master? (y or n):
```

- If you answer **y** for yes, security will be enabled and you will be taken to the Security Options Menu.
- If you answer **n** for no, all security settings (except FTP security) will remain disabled and you will be taken back to the Main Security Menu.

The Security Options Menu is displayed as follows:

```
Select to change current security option
 1) Terminal (RS232) Security.................. Enabled
 2) HTTP Security.............................. Enabled
 3) Telnet Security............................ Enabled
 4) Security Configuration Security............ Enabled
Or <ENTER> to return to previous menu

Security Options ->
```

The selection listed will display what the current settings. To change an option, select the number listed next to the option.

For example, if selection **2)** is selected, HTTP Security will be disabled. The menu will then be displayed again as follows:

```
Select to change current security option
 1) Terminal (RS232) Security.................. Enabled
 2) HTTP Security.............................. Disabled
 3) Telnet Security............................ Enabled
 4) Security Configuration Security............ Enabled
Or <ENTER> to return to previous menu

Security Options ->
```

Each selection simply toggles the security setting selected. Press <ENTER> to exit the menu and return to the Main Security Menu.

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

The items in the Security Options Menu are described below:

Security Options Menu	
Command	**Description**
`1) Terminal (RS232) Security (Enabled/Disabled)`	This selection enables/disables Terminal (RS232 Program port) Security. If Terminal Security is enabled, a user must have sufficient access rights to login to a Terminal session.
`2) HTTP Security (Enabled/Disabled)`	This selection enables/disables HTTP (Web Server) Security. If HTTP Security is enabled, a user must have sufficient access rights to browse to the NetLinx Master with a Web Browser.
`3) Telnet Security (Enabled/Disabled)`	This selection enables/disables Telnet Security. If Telnet Security is enabled, a user must have sufficient access rights to login to a Telnet session.
`4) Security Configuration Security (Enabled/Disabled)`	This selection enables/disables Security Configuration Security. If Security Configuration Security is enabled, a user must have sufficient access rights to access the Main Security Menu.

Option 2 - Display system security options for NetLinx Master

Type **2** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to display the current security options, and their current state (`Enabled/Disabled`). For example:

```
Master Security.....................Disabled
Terminal............................Disabled
HTTP................................Disabled
Telnet..............................Disabled
Security/Configuration..............Disabled

Press <ENTER> key to continue
```

Option 3 - Add user

1. Type **3** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to create a new user account. A sample session response is:

```
The following users are currently enrolled:
administrator
Fred
Betty

Enter user name:
```

2. At the **`Enter user name`** prompt, enter a new user name (for example "`Bilbo`"). A user name is a valid character string (4 - 20 alpha-numeric characters) defining the user. This string is ***case sensitive***. Each user name must be unique.
3. Press <ENTER> to enter the new user name. The session then prompts you for a password for the new user.

4. Enter a password for the new user. A password is a valid character string (4 - 20 alpha-numeric characters) to supplement the user name in defining the potential client. This string is also ***case sensitive***.
5. The session then prompts you to verify the new password. Enter the password again, and press <ENTER>.
6. Assuming the password was verified, the session then displays the Edit User menu (*see below*).

Option 4 - Edit User

1. Type **4** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to edit an existing user account. A sample session response is:

```
Select from the following list of enrolled users:

1) administrator
2) Fred
3) Betty
4) Bilbo
Select User:
```

2. Select the user account (1-X) that you want to edit, and press <ENTER> to display the Edit User Menu (described below).

Any changes made via the Edit User menu will affect the selected user account.

Edit User Menu

The Edit User Menu is accessed whenever you enter the Add user, or Edit user selections from the Main Security Menu. The Edit User Menu is displayed as follows:

```
Please select from the following options:

 1) Change User Password
 2) Change Inherits From Group
 3) Add Directory Association
 4) Delete Directory Association
 5) List Directory Associations
 6) Change Access Rights
 7) Display User Record Contents
Or <ENTER> to return to previous menu

Edit User ->
```

Each selection (1-7) accesses the named option. Press <ENTER> by itself to exit the menu and return to the Main Security Menu.

The Edit User Menu options are described in the following table:

Edit User Menu	
Command	**Description**
`1) Change User Password`	This selection prompts you to enter the new password (twice) for the user. Once the new password is entered, the user must use the new password from that point forward.
`2) Change Inherits From Group`	This selection will display the current group the user is assigned to (if any). It will then display a list of current groups and prompts you to select the new group.
`3) Add Directory Association`	This selection will display any current Directory Associations assigned to the user, and then will prompt you for a path for the new Directory Association. Refer to *Directory Associations on page 35* for details.
`4) Delete Directory Association`	This selection will display any current Directory Associations assigned to the user, and then will prompt you to select the Directory Association you want to delete.
`5) List Directory Associations`	This selection will display any current Directory Associations assigned to the user.
`6) Change Access Rights`	This selection will display access the Access Rights Menu for the user, which allows you to set the rights assigned to the user.
`7) Display User Record Contents`	This selection will display the group the user is assigned to and the current Access Rights assigned to the user.

Access Rights Menu

The Access Rights Menu is accessed whenever you select Change Access Rights from the Edit User Menu, or Change Access Rights from the Edit Group Menu. The Access Rights Menu is displayed as follows:

```
Select to change current access right
 1) Terminal (RS232) Access.................. Disabled
 2) Admin Change Password Access............. Disabled
 3) FTP Access............................... Disabled
 4) HTTP Access.............................. Enabled
 5) Telnet Access............................ Enabled
 6) Security Configuration Access............ Enabled
Or <ENTER> to return to previous menu
Set Rights ->
```

The selection listed will display the current access rights. Each selection simply toggles the access right selected. Press <ENTER> to exit the menu and return to the previous menu.

The Access Rights Menu is described in the following table:

Access Rights Menu	
Command	**Description**
1) Terminal (RS232) Access (Enable/Disable)	Enables/disables Terminal (RS232 Program port) Access. The account has sufficient access rights to login to a Terminal session if this option is enabled.
2) Admin Change Password Access (Enable/Disable)	Enables/disables Administrator Change Password Access. The account has sufficient access rights to change the administrator password if this option is enabled.
3) FTP Access (Enable/Disable)	Enables/disables FTP Access. The account has sufficient access rights to access the NetLinx Master's FTP Server if this option is enabled.
4) HTTP Access (Enable/Disable)	This selection enables/disables HTTP (Web Server) Access. The account has sufficient access rights to browse to the NetLinx Master with a Web Browser if this option is enabled.
5) Telnet Access (Enable/Disable)	This selection enables/disables Telnet Access. The account has sufficient access rights to login to a Telnet session if this option is enabled.
6) Security Configuration Access (Enable/Disable)	This selection enables/disables Security Configuration Access. The account has sufficient access rights to access the Main Security Menu if this option is enabled.

Option 5 - Delete user

1. Type **5** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to delete an existing user account. A sample session response is:

```
Select from the following list of enrolled users:
1) Fred
2) Betty
3) Bilbo
Select User ->
```

2. Select the user to delete and press <ENTER> to delete the user account, and return to the Security Setup menu.

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Option 6 - Show the list of authorized users

1. Type **6** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to view a list of currently enrolled users.
2. Press <ENTER> to return to the Security Setup menu.

Option 7 - Add Group

1. Type **7** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to add a group account. A sample session response is:

```
The following groups are currently enrolled:
administrator

Enter name of new group:
```

2. Enter a name for the group. A group name is a valid character string (4 - 20 alpha-numeric characters) defining the group. This string is ***case sensitive***, and each group name must be unique.
3. Press <ENTER> to display the following Edit Group menu:

Edit Group Menu

```
Please select from the following options:
1) Add directory association
2) Delete directory association
3) List directory associations
4) Change Access rights
5) Display Access Rights
Or <ENTER> to return to previous menu.
Edit Group ->
```

Edit Group Menu: Add directory association

1. At the Edit Group prompt, type **1** to add a new directory association. A sample session response is:

```
There are currently no directories associated with this account
New directory:
```

A Directory Association is a path that defines the directories and/or files that a particular user or group can access via the HTTP (Web) Server on the NetLinx Master. This character string can range from 1 to 128 alpha-numeric characters. This string is ***case sensitive***. This is the path to the file or directory you want to grant access. Access is limited to the user (i.e. doc:user) directory of the master. All subdirectories of the user directory can be granted access.

A single '/' is sufficient to grant access to all files and directories in the user directory and it's sub-directory. The '*' wildcard can also be added to enable access to all files. All entries should start with a '/'. Here are some examples of valid entries:

Path	Notes
`/`	Enables access to the user directory and all files and subdirectories in the user directory.
`/*`	Enables access to the user directory and all files and subdirectories in the user directory.
`/user1`	If `user1` is a file in the user directory, only the file is granted access. If `user1` is a subdirectory of the user directory, all files in the `user1` and its sub-directories are granted access.
`/user1/`	`user1` is a subdirectory of the user directory. All files in the `user1` and its sub-directories are granted access.
`/Room1/iWebControlPages/*`	`/Room1/iWebControlPages` is a subdirectory and all files and its subdirectories are granted access.
`/results.txt`	`results.txt` is a file in the user directory and access is granted to that file.

By default, all accounts that enable HTTP Access are given a '`/*`' Directory Association if no other Directory Association has been assigned to the account.

When you are prompted to enter the path for a Directory Association, the NetLinx Master will attempt to validate the path. If the directory or file is not valid (i.e. it does not exist at the time you entered the path), the NetLinx Master will ask you whether you were intending to grant

access to a file or directory. From the answer, it will enter the appropriate Directory Association. The NetLinx Master will not create the path if it is not valid. That must be done via another means, most commonly by using an FTP client and connecting to the FTP server on the NetLinx Master.

Edit Group menu: Delete directory association

1. At the Edit Group prompt, type **2** to delete an existing directory association. A sample session response is:

```
Select a directory association from the following:
1) /directory1/*
2) /directory2/*
Select Directory ->
```

2. Select the directory association to be deleted, and press <ENTER> to delete the directory association, and return to the Edit Group menu.

Edit Group menu: List directory associations

1. At the Edit Group prompt, type **3** to list all existing directory associations. A sample session response is:

```
The following directory associations are enrolled:
/directory1/*
/directory2/*

Press <ENTER> key to continue
```

2. Press <ENTER> to return to the Edit Group menu.

Edit Group menu: Change Access Rights

1. At the Edit Group prompt, type **4** to change the current access rights for the selected group account. A sample session response is:

```
Select to change current access right:
1) Terminal (RS232) Access...................Disabled
2) Admin Change Password Access..............Disabled
3) FTP Access................................Disabled
4) HTTP Acccess..............................Disabled
5) Telnet Access.............................Disabled
6) Security Configuration Access.............Disabled
or <ENTER> to return to previous menu

Set Rights ->
```

2. Each selection simply toggles the security setting selected. <ENTER> is entered by itself to exit the menu and return to the Main Security Menu.

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Edit Group menu: Display Access Rights

1. At the Edit Group prompt, type **5** to view the current access rights for the selected group account. A sample session response is:

```
Terminal (RS232)...................Disabled
Admin Password Change..............Disabled
FTP................................Disabled
HTTP...............................Disabled
Telnet.............................Disabled
Security Configuration.............Disabled

Press <ENTER> key to continue
```

2. Press <ENTER> to return to the Edit Group menu.

Option 8 - Edit Group

1. Type **8** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to edit an existing group account. A sample session response is:

```
Select from the following list:
1) administrator
2) Group 1
3) Group 2
Select group ->
```

2. Select a group from the list of currently enrolled groups and press <ENTER> to open the Edit Group Menu. This is the same Edit Group Menu that was access via the Add Group option:

```
1) Add directory association
2) Delete directory association
3) List directory associations
4) Change Access rights
5) Display Access Rights
```

This menu is described on the previous pages (see *Edit Group Menu on page 80*).

Option 9 - Delete Group

1. Type **9** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to delete an existing group account. A sample session response is:

```
Select from the following list:
1) Group 1
2) Group 2
Select group ->
```

2. Select the group account to be deleted, and press <ENTER> to delete the group and return to the Security Setup menu.

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Option 10 - Show List of Authorized Groups

1. Type **10** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to display a list of all authorized group accounts. A sample session response is:

```
The following groups are currently enrolled:
administrator
Group 1

Press <ENTER> key to continue
```

2. Press <ENTER> to return to the Security Setup Menu.

Option 11 - Set Telnet Timeout in seconds

This feature is disabled after the installation of firmware build 130 or higher onto your target Master.

1. Type **11** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to set the Telnet Timeout value, in seconds. A sample session response is:

```
Specify Telnet Timeout in seconds:
```

2. Enter the number of seconds before you want The Telnet session to timeout, and press <ENTER> to return to the Security Setup Menu.

Option 12 - Display Telnet Timeout in seconds

This feature is disabled after the installation of firmware build 130 or higher onto your target Master.

1. Type **12** and <ENTER> at the Security Setup prompt (at the bottom of the Main Security Menu) to view the current Telnet Timeout value (in seconds). A sample session response is:

```
Telnet Timeout is 10 seconds.
```

2. Press <ENTER> to return to the Security Setup Menu.

Option 13 - Make changes permanent by saving to flash

When changes are made to the security settings of the master, they are initially only changed in RAM and are not automatically saved permanently into flash. This selection saved the current security settings into flash. Also, if you attempt to exit the Main Security Menu and the security settings have changed but not made permanent, you will be prompted to save the settings at that time.

Type **13** and <ENTER> at the Security Setup prompt to (permanently) save all changes to flash.

Changes made to the target Master from within the Terminal window are not reflected within the web browser, until the Master is rebooted and the web browser connection is refreshed.
Any changes made to the Master, from within the web browser are instantly reflected within the Terminal session without the need to reboot.

Main Security Menu

The Main Security menu is described below:

Main Security Menu	
Command	**Description**
1) Set system security options for NetLinx Master	This selection will bring up the Security Options Menu that allows you to change the security options for the NetLinx Master (refer to the *Security Options Menu* section on page 76 for details). These are "global" options that enable rights given to users and groups. For instance, if you want to disable Telnet security for all users, you would simply go to this menu and disable Telnet security for the entire master. This would allow any user, whether they have the rights to Telnet or not. These options can be thought of as options to turn on security for different features of the NetLinx Master.
2) Display system security options for NetLinx Master	This selection will display the current security options for the NetLinx Master.
3) Add user	This selection will prompt you for a user name and password for a user you would like to create. After the user is added, you will be taken to the Edit User Menu to setup the new users rights (see the *Edit User Menu* section on page 78 for details).
4) Edit user	This selection will prompt you select a user. Once you have selected the user you want to edit, it will take you to the Edit User Menu so you can edit the user's rights (see the *Edit User Menu* section on page 78 for details).
5) Delete user	This selection will prompt you select a user to delete.
6) Show the list of authorized users	This selection displays a list of users.
7) Add group	This selection will prompt you for a group name fro a group you would like to create. After the group is added, you will be taken to the Edit Group Menu to setup the new users right (see the *Edit Group Menu* section on page 80 for details).
8) Edit group	This selection will prompt you select a group. Once you have selected the group you want to edit, it will take you to the Edit Group Menu so you can edit the group's rights (see the *Edit Group Menu* section on page 80 for details).
9) Delete group	This selection will prompt you select a group to delete. A group can only be deleted if there are no users assigned to that group.
10) Show list of authorized groups	This selection displays a list of groups.
11) Set Telnet Timeout in seconds	This selection allows you to set the time a telnet session waits for a user to login. When a Telnet client connects to the NetLinx Master, it is prompted for a user name. If the client does not enter a users name for the length of time set in this selection, the session will be closed by the NetLinx Master.
12) Display Telnet Timeout in seconds	This selection allows you to display the time a telnet session waits for a user to login.
13) Make changes permanent by saving to flash	When changes are made to the security settings of the master, they are initially only changed in RAM and are not automatically saved permanently into flash. This selection saved the current security settings into flash. Also, if you attempt to exit the Main Security Menu and the security settings have changed but not made permanent, you will be prompted to save the settings at that time.

Main Security Menu (Cont.)	
Command	**Description**
14) Reset Database	If a user has been given "administrator rights", this additional menu option is displayed. This selection will reset the security database to its Default Security Configuration settings, erasing all users and groups that were added. This is a permanent change and you will be asked to verify this before the database is reset.
15) Display Database	If a user has been given "administrator rights", this additional menu option is displayed. This selection will display the current security settings to the terminal (excluding user passwords).

Default Security Configuration

By default, the NetLinx Master will create the following accounts, access rights, directory associations, and security options.

```
Account 1:              User Name: administrator
Password:               password
Group:                  administrator
Rights:                 All
Directory Association: /*

Account 2:              User Name: NetLinx
Password:               password
Group:                  none
Rights:                 FTP Access
Directory Association: none

Group 1:                Group: administrator
Rights:                 All
Directory Association: /*

Security Options:       FTP Security Enabled
                        Admin Change Password Security Enabled
                        All other options disabled
```

- The ***administrator*** user account cannot be deleted or modified with the exception of its password. Only a user with "Change Admin Password Access" rights can change the administrator password.
- The ***NetLinx*** user account is created to be compatible with previous NetLinx Master firmware versions.
- The ***administrator*** group account cannot be deleted or modified.
- The FTP Security and Admin Change Password Security are always enabled and cannot be disabled.

Help menu

Type **help** at the prompt in the Telnet session to display the following help topics:

Help Menu Options	
Command	**Description**
----- Help ----- <D:P:S>	(Extended diag messages are OFF) <D:P:S>: Device:Port:System. If omitted, assumes master.
? or Help	Displays this list.
DATE	Displays the current date.
DEVICE HOLDOFF ON|OFF	Sets the master to holdoff devices (i.e. does not allow them to report ONLINE) until the NetLinx program has completed executing the DEFINE_START section. If set to ON, any messages to devices in DEFINE_START will be lost, however, this prevents incoming messages being lost in the master upon startup. When DEVICE_HOLDOFF is ON, you must use ONLINE events to trigger device startup SEND_COMMANDs. By default, DEVICE HOLDOFF is OFF to maintain compatibility with Axcess systems where **f** devices are initialized in DEFINE_START.
DEVICE STATUS <D:P:S>	Provides information about the specified device.
DNS LIST <D:P:S>	Displays the DNS configuration of a device.
DISK FREE	Displays the amount of free space on the disk.
GET DEVICE HOLDOFF	Displays the state of the device holdoff setting in the master
GET IP <D:P:S>	Displays the IP configuration of a device.
HELP SECURITY	Displays security related commands.
IP STATUS	Provides information about NetLinx IP Connections.
MEM	Shows size of the largest block of available memory.
MSG ON|OFF	Enables/Disables extended diagnostic messages.
OFF [D:P:S or NAME,CHAN]	Turns off the specified channel.
ON [D:P:S or NAME,CHAN]	Turns on the specified channel.
PASS [D:P:S or NAME]	Puts the Session in pass mode to the specified device. • Mode is exited by ++ ESC ESC. • Display Format is set by ++ ESC n If n is A, format = ASCII If n is D, format = Decimal If n is H, format = Hex
PING [ADDRESS]	Pings an address (IP or URL). Specify -a option for reverse lookup.
PROGRAM INFO	Displays a list of program modules loaded.
PULSE [D:P:S or NAME,CHAN]	Pulses the specified channel.
REBOOT <D:P:S>	Reboots the device.
RELEASE DHCP	Releases the current DHCP lease.
ROUTE MODE DIRECT|NORMAL	Set the Master-Master route mode.
SEND_COMMAND D:P:S or NAME,COMMAND	Sends the specified command to the device.The Command uses NetLinx string syntax. • Ex: send_command 1:1:1,"'This is a test',13,10" • Ex: send_command RS232_1,"'This is a test',13,10"
SEND_STRING D:P:S or NAME,STRING	Sends the specified string to the device.
SET DATE	Set the current date.

Help Menu Options (Cont.)	
Command	**Description**
SET DNS <D:P:S>	Setup the DNS configuration of a device.
SET ICSP PORT	Sets the IP port listened to for ICSP connections.
SET ICSP TCP TIMEOUT	Sets the timeout period for ICSP and i!-WebControl TCP connections.
SET IP <D:P:S>	Setup the IP configuration of a device.
SET TELNET PORT	Sets the IP port listened to for telnet connections.
SET THRESHOLD	Sets the master's internal message thresholds.
SET TIME	Set the current time.
SET URL <D:P:S>	Setup the initiated connection list URLs of a device.
SHOW COMBINE	Displays a list of devices, levels, and channels that are currently combined.
SHOW DEVICE <D:P:S>	Displays a list of devices connected and attributes.
SHOW LOG <START>	Display the message log. <start> specifies message to begin the display. 'all' will display all messages.
SHOW NOTIFY	Display the Notify Device List (Master-Master).
SHOW REMOTE	Displays the Remote Device List (Master-Master).
SHOW ROUTE	Displays the Master's routing information.
SHOW SYSTEM <S>	Displays a list of devices in a system.
TCP LIST	Displays a list of active TCP connections.
TIME	Display the current time.
URL LIST <D:P:S>	Display the initiated connection list URLs of a device.
SSL SECURITY ENABLE:DISABLED	Enables or Disables the Web Server SSL security.

Logging Into a Session

Until Telnet security is enabled, a session will begin with a welcome banner.

```
Welcome to NetLinx v2.10.80 Copyright AMX Corp. 1999-2004
>
```

The welcome banner is not displayed for Terminal sessions.

When Terminal security is enabled, the user will be prompted for a user name and password before they will be allowed to access any commands available from Telnet. No welcome banner will be displayed until a valid login is made. When the session is started, the user will see a login prompt as seen below:

```
Login:
```

The user (Login) name is case sensitive. The user name must be entered with the exact combination of upper and lower letters as was assigned to them by the security administrator. The user name must be at least 4 characters long and no more than 20 characters. Any combination of letters, numbers, or other characters may be used.

The user would enter their user name and then would be prompted for a password:

```
Login: User1
Password:
```

The password is case sensitive. The password must be entered with the exact combination of upper and lower letters as was assigned to them by the security administrator. The password must be at least 4 characters long and no more than 20 characters. Any combination of letters, numbers, or other characters may be used.

After the password is entered, if the password is correct you will see a welcome banner as shown below:

```
Login: User1
Password: *****
Welcome to NetLinx v2.10.80 Copyright AMX Corp. 1999-2002
>
```

If the password is incorrect, the following will be displayed:

```
Login: User1
Password: *****
Login not authorized.  Please try again.
```

After a delay, another login prompt will be displayed to allow the user to try again. If after 5 prompts, the login is not done correctly the following will be displayed and the connection closed:

```
Login not allowed.  Goodbye!
```

If a user opens a connection but does not enter a user name or password (i.e. they just sit at a login prompt), the connection will be closed after 1 minute.

Logout

The logout command will log the user out of the current secure telnet session. For a Terminal session, the user will be logged out and to access Terminal commands again the user will first have to login.

Help Security

The help security command will display the security menu as shown previously.

Setup Security

The security command displays a series of menus that allow the security administrator to create and edit users, create and edit groups, and setup directory associations for the Web Server. A user must be given rights to access this command. Any user that does not have rights to Security Configuration will see the following message when trying to access the setup security command:

```
>setup security
You are not authorized to access security commands
```

If a user is authorized, or if Security Configuration security is not enabled, the Main Security Menu will be displayed.

Programming

The NetLinx programming language allows numbers in the range 0-32,767. Device 0 refers to the Master Card; numbers greater than 32,767 are reserved for internal use only.

The NetLinx programming language requires a Device:Port:System (D:P:S) syntax where Axcess expects only a device number. The NetLinx D:P:S triplet variable is expressed as:

```
DEVICE:PORT:SYSTEM
```

where:

- Device: 16-bit integer representing the device number (0-32,767). 0 = the local Master.
- Port: 16-bit integer representing the port number (in the range 1 through the number of ports on the NetLinx Master or device).
- System: 16-bit integer representing the system number (0 = this system).

Program Port Commands

The Program port commands listed in the Program Port Commands table below can be sent directly to the Master Card using a terminal program (i.e. Telnet). In order for Telnet to be effective, you must initiate a session with the master. Be sure that your PC's COM port and terminal program's communication settings match those in the following table.

PC COM Port Communication Settings	
Baud	38400 (default)
Parity	none
Data Bits	8
Stop Bits	1
Flow Control	none

In your terminal program, type "`Help`" or a "`?`" <Enter> to display the Program port commands listed below.

Program Port Commands	
Command	**Description**
`ECHO OFF`	Disables terminal character's echo (display) function.
`ECHO ON`	Enables terminal character's echo (display) function.

`DATE`	Displays the current date and day of the week.
	Example:
	`>DATE`
	`10/31/2001 Wed`

Program Port Commands (Cont.)	
Command	**Description**

SET DATE	Prompts you to enter the new date for the Master Card.
	When the date is set on the Master Card, the new date will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the date on any system device, the new date will be reflected on the system's Master, and on all connected devices.
	This will not update clocks on devices connected to another Master (in Master-to-Master systems).
	Example:
	`>SET DATE`
	`Enter Date: (mm/dd//yyyy) ->`

TIME	Displays the current time on the Master Card.
	Example:
	`>TIME`
	`13:42:04`

SET TIME	Prompts you to enter the new time for the Master Card.
	When the time is set on the Master Card, the new time will be reflected on all devices in the system that have clocks (i.e. touch panels). By the same token, if you set the time on any system device, the new time will be reflected on the system's Master, and on all connected devices.
	This will not update clocks on devices connected to another Master (in Master-to-Master systems).
	Example:
	`>SET TIME`
	`Enter Date: (hh:mm:ss) ->`

DEVICE STATUS <D:P:S>	Displays a list of all active (on) channels for the specified D:P:S. Enter DEVICE STATUS without the D:P:S variable, the Master Card displays ports, channels, and version information.
	Displays status of the specified Master.
	Example (on a local Master):
	`>DEVICE STATUS [0:1:0]`
	`Device 0 AMX Corp.,Master,v2.10.75 contains 1 Ports.`
	`Port 1 - Channels:256 Levels:8`
	`MaxStringLen=64 Types=8 bit MaxCommandLen=64 Types=8 bit`
	`The following input channels are on:None`
	`The following output channels are on:None`
	`The following feedback channels are on:None`
	`Level 1=0 Supported data types=UByte,UInt`
	`Level 2=0 Supported data types=UByte,UInt`
	`Level 3=0 Supported data types=UByte,UInt`
	`Level 4=0 Supported data types=UByte,UInt`
	`Level 5=0 Supported data types=UByte,UInt`
	`Level 6=0 Supported data types=UByte,UInt`
	`Level 7=0 Supported data types=UByte,UInt`
	`Level 8=0 Supported data types=UByte,UInt`

DNS LIST <D:P:S>	Displays:
	• Domain suffix·
	• Configured DNS IP Information
	Example:
	`>DNS LIST [0:1:0]`
	`Domain suffix:amx.com`
	`The following DNS IPs are configured`
	`Entry 1-192.168.20.5`
	`Entry 2-12.18.110.8`
	`Entry 3-12.18.110.7`

Program Port Commands (Cont.)	
Command	**Description**

DISK FREE	Displays the total bytes of free space available on the Master Card's compact Flash memory.
	Example:
	`>DISK FREE`
	`The disk has 2441216 bytes of free space.`

GET IP <D:P:S>	Displays the Master Card's D:P:S, Host Name, Type (DHCP or Static), IP Address, Subnet Mask, Gateway IP, and MAC Address.
	Example:
	`>GET IP [0:1:50]`
	`IP Settings for 0:1:50`
	`HostName MLK_INSTRUCTOR`
	`Type DHCP`
	`IP Address 192.168.21.101`
	`Subnet Mask 255.255.255.0`
	`Gateway IP 192.168.21.2`
	`MAC Address 00:60:9f:90:0d:39`

MEM	Displays the largest free block of Master Card memory.
	Example:
	`>MEM`
	`The largest free block of memory is 11442776 bytes.`

MSG ON or MSG OFF	MSG On sets the terminal program to display all messages generated by the Master Card. MSG OFF disables the display.
	Example:
	`> MSG ON`
	`Extended diagnositic information messages turned on.`
	`> MSG OFF`
	`Extended diagnositic information messages turned off.`

OFF <D:P:S, channel>	Turns off a channel on a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system, or the name of the device that is defined in the DEFINE_DEVICE section of the program.
	Syntax:
	`OFF[name,channel]`
	-or-
	`OFF[D:P:S,channel]`
	Example:
	`>OFF[5001:7:4]`
	`Sending Off[5001:7:4]`

ON <D:P:S, channel>	Turns on a channel on a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the program.
	Syntax:
	`ON[name,channel]`
	or
	`ON[D:P:S,channel]`
	Example:
	`>ON[5001:7:4]`
	`Sending On[5001:7:4]`

Program Port Commands (Cont.)	
Command	**Description**

PASS <D:P:S>	Sets up a pass through mode to a device. In pass through mode, any string received by the device is displayed on the screen, and anything typed is sent as a string to the device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system, or the name of the device that is defined in the DEFINE_DEVICE section of the program.
	Example:
	`>pass[5001:7:4]`
	`Entering pass mode.`
	To exit pass mode, type + + esc esc.

PING <IP ADDRESS>	Tests network connectivity to and confirms the presence of another networked device. The syntax is just like the PING application in Windows or Linux.
	Example:
	`>ping 192.168.21.209`
	`192.168.21.209 is alive.`

PROGRAM INFO	Displays the name of the NetLinx program residing in the Master Card.
	Example:
	`>PROGRAM INFO`
	`-- Program Name Info`
	`-- Module Count = 1`
	`1 Name is i!-PCLinkPowerPointTest`
	`-- File Names = 2`
	`1 = C:\Program Files\AMX Applications\i!-PCLinkPowerPoint`
	`2 = C:\Program Files\Common Files\AMXShare\AXIs\NetLinx.axi`
	`2 = Name is MDLPP`
	`-- File Names = 2`
	`1 C:\AppDev\i!-PCLink-PowerPoint\i!-PCLinkPowerPointMod.axs`
	`2 C:\Program files\Common Files\AMXShare\AXIs\NetLinx.axi`

PULSE <D:P:S, channel>	Pulses a channel on a device on and off. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the program.
	Example:
	`>PULSE[50001:8:50,1]`
	`Sending Pulse[50001:8:50,1]`

REBOOT <D:P:S>	Reboots the Master Card or specified device.
	Example:
	`>REBOOT [0:1:0]`
	`Rebooting...`

RELEASE DHCP	Releases the DHCP setting for the Master Card.
	Example:
	`>RELEASE DHCP`
	`The Master must be rebooted to acquire a new DHCP lease.`

Program Port Commands (Cont.)	
Command	**Description**

ROUTE MODE DIRECT|NORMAL	Sets the Master-to-Master route mode:
	• Normal mode - allows a Master to communicate with any Master accessible via the routing tables (shown with the SHOW ROUTE command). This includes a directly-connected Master (route metric =1) and indirectly connected masters (route metric greater than 1, but less than 16).
	• Direct mode - allows communication only with masters that are directly connected (route metric = 1). Indirectly connected masters cannot be communicated within this mode.
	Examples:
	`>ROUTE MODE DIRECT`
	`Route Mode "Direct" Set`
	`>ROUTE MODE NORMAL`
	`Route Mode "Normal" Set`

SEND_COMMAND <D:P:S>	Sends a command to a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device that is defined in the DEFINE_DEVICE section of the NetLinx Program. The data of the string is entered with NetLinx string syntax.
SEND_STRING <D:P:S>	Sends a string to a device. The device can be on any system the Master you are connected to can reach. You can specify the device number, port, and system; or the name of the device defined in the DEFINE_DEVICE section of the NetLinx Program. The data of the string is entered with NetLinx string syntax.

SET DNS <D:P:S>	Prompts you to enter a Domain Name, DNS IP #1, DNS IP #2, and DNS IP #3. Then, enter Y (yes) to approve/store the information in the Master Card. Entering N (no) cancels the operation.
	Example:
	`>SET DNS [0:1:0]`
	`-- Enter New Values or just hit Enter to keep current settings --`
	
	`Enter Domain Suffix: amx.com`
	`Enter DNS Entry 1 : 192.168.20.5`
	`Enter DNS Entry 2 : 12.18.110.8`
	`Enter DNS Entry 3 : 12.18.110.7`
	
	`You have entered: Domain Name: amx.com`
	`DNS Entry 1: 192.168.20.5`
	`DNS Entry 2: 12.18.110.8`
	`DNS Entry 3: 12.18.110.7`
	
	`Is this correct? Type Y or N and Enter -> Y`
	`Settings written. Device must be rebooted to enable new settings`

SET IP <D:P:S>	Prompts you to enter a Host Name, Type (DHCP or Fixed), IP Address, Subnet Mask, and Gateway IP Address.
	Enter Y (yes) to approve/store the information in the Master Card.
	Entering N (no) cancels the operation.
	Example:
	`>SET IP [0:1:0]`
	`--- Enter New Values or just hit Enter to keep current settings ---`
	
	`Enter Host Name: MLK_INSTRUCTOR`
	`Enter IP type. Type D for DHCP or S for Static IP and then Enter: DHCP`
	`Enter Gateway IP: 192.168.21.2`
	
	`You have entered: Host Name MLK_INSTRUCTOR`
	`Type DHCP`
	`Gateway IP 192.168.21.2`
	`Is this correct? Type Y or N and Enter -> y`
	`Settings written. Device must be rebooted to enable new settings.`

Program Port Commands (Cont.)	
Command	**Description**

SET URL <D:P:S>	Prompts you to enter the URL address and port number of another Master or device (that will be added to the URL list). Then, enter Y (yes) to approve/store the new addresses in the Master Card.
	Entering N (no) cancels the operation.
	Example:
	`>SET URL [0:1:0]`
	`No URLs in the URL connection list`
	`Type A and Enter to Add a URL or Enter to exit. -> a`
	
	`Enter URL -> 192.168.21.200`
	`Enter Port or hit Enter to accept default (1319) ->`
	`Enter Type (Enter for permanent or T for temporary) ->`
	`URL Added successfully.`

SHOW COMBINE	Displays a list of any combined devices.
	Example:
	`> SHOW COMBINE`
	`Combines`
	`--------`
	`Combined Device([33096:1:1],[96:1:1])`
	`Combined Level([33096:1:1,1],[128:1:1,1],[10128:1:1,1])`
	`Combined Device([33128:1:1],[128:1:1],[10128:1:1])`

SHOW DEVICE <D:P:S>	Displays a list of all devices present on the bus.
	Example:
	`>SHOW DEVICE [0:1:0]`
	`Local devices for system #50 (This System)`
	`----------`
	`Device (ID)Model (ID)Mfg FWID Version`
	`00000 (00256)Master (00001)AMX Corp. 00256 v2.10.75`
	`(PID=0:OID=0) Serial='2010-12090',0,0,0,0,0,0`
	`Physical Address=NeuronID 000239712501`
	`(00256)vxWorks Image (00001) 00257 v2.00.77`
	`(PID=0:OID=1) Serial=N/A`
	`(00256)BootROM (00001) 00258 v2.00.76`
	`(PID=0:OID=2) Serial=N/A`
	`(00256)AXLink I/F uContr(00001) 00270 v1.02`
	`(PID=0:OID=3) Serial=0000000000000000`
	`00096 (00192)VOLUME 3 CONTROL BO(00001)AMX Corp. 00000 v2.10`
	`(PID=0:OID=0) Serial=0000000000000000`
	`Physical Address=Axlink`
	`00128 (00188)COLOR LCD TOUCH PAN(00001)AMX Corp. 32778 v5.01d`
	`(PID=0:OID=0) Serial=0000000000000000`
	`Physical Address=Axlink`
	`05001 (00257)NXI Download (00001)AMX Corp. 00260 v1.00.20`
	`(PID=0:OID=0) Serial=0,0,0,0,0,0,0,0,0,0,0,0,`
	`Physical Address=NeuronID 000189145801`
	`(00257)NXI/NXI-1000 Boot(00001) 00261 v1.00.00`
	`(PID=0:OID=1) Serial=0,0,0,0,0,0,0,0,0,0,0,0,`
	`10002 (00003)PHAST PLK-IMS (00001)Phast Corp. 00003 v3.12`
	`(PID=0:OID=0) Serial=0000000000000000`
	`Physical Address=NeuronID 0100417BD800`

Program Port Commands (Cont.)	
Command	**Description**
SHOW LOG	Displays the log of messages stored in the Master's memory. The Master logs all internal messages and keeps the most recent messages. The log contains:· • Entries starting with first specified or most recent • Date, Day, and Time message was logged • Which object originated the message • The text of the message SHOW LOG [start] [end] SHOW LOG ALL If start is not entered, the most recent message will be first. If end is not entered, the last 20 messages will be shown. If ALL is entered, all stored messages will be shown, starting with the most recent. Example: >SHOW LOG Message Log for System 50 Version: v2.10.75 Entry Date/Time Object Text --- 1: 11-01-2001 THU 14:14:49 ConnectionManager Memory Available = 11436804 <26572> 2: 11-01-2001 THU 14:12:14 ConnectionManager Memory Available = 11463376 <65544> 3: 11-01-2001 THU 14:10:21 ConnectionManager Memory Available = 11528920 <11512> 4: 11-01-2001 THU 14:10:21 TelnetSvr Accepted Telnet connection:socket=14 addr=192.168.16.110 port=2979 5: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 10002:1:50 6: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 128:1:50 7: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OffLine 128:1:50 8: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 96:1:50 9: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OffLine 96:1:50 10: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 128:1:50 11: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 96:1:50 12: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:16:50 13: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:15:50 14: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:14:50 15: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:13:50 16: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:12:50 17: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:11:50 18: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:10:50 19: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:9:50 20: 11-01-2001 THU 14:05:51 Interpreter CIpEvent::OnLine 5001:8:50
SHOW NOTIFY	Displays a list of devices (up to 1000) that other systems have requested input from and the types of information needed. Example: >SHOW NOTIFY Device Notification List of devices requested by other Systems Device:Port System Needs --- 00128:00001 00108 Channels Commands Strings Levels 33000:00001 00108 Channels Commands

Program Port Commands (Cont.)	
Command	**Description**

SHOW REMOTE	Displays a list of the devices this system requires input from and the types of information needed. If when a NetLinx Master connects to another NetLinx Master, the newly connecting system has a device that the local system desires input from; the new system is told what information is desired from what device.
	Example:
	`>SHOW REMOTE`
	
	`Device List of Remote Devices requested by this System`
	
	`Device Port System Needs`
	`---------- ---------- ---------- ----------`
	`00001 00001 00001 Channels Commands`
	`00002 00001 00001 Channels Commands`
	`33000 00001 00001 Channels Commands`
	`00128 00001 00108 Channels Commands Strings Levels`
	`33000 00001 00108 Channels Commands`

SHOW ROUTE	Displays information about how this NetLinx Master is connected to other NetLinx masters.
	Example:
	`>SHOW ROUTE`
	`Route Data:`
	
	`System Route Metric PhyAddress`
	`---------- ---------- ---------- ----------`
	`-> 50 50 0 Axlink`

SHOW SYSTEM	Provides a list of all devices in all systems currently on-line. The systems lists are either directly connected to this Master (i.e. 1 hop away), or are referenced in the DEFINE_DEVICE section of the NetLinx program. Optionally, you may provide the desired system number as a parameter to display only that system's information (e.g. SHOW SYSTEM 2001). The systems listed are in numerical order.
	Example:
	`>SHOW SYSTEM`
	`Local devices for system #50 (This System)`
	`---------- ----------`
	`Device (ID)Model (ID)Mfg FWID Version`
	`00000 (00256)Master (00001)AMX Corp. 00256 v2.10.75`
	`(PID=0:OID=0) Serial='2010-12090',0,0,0,0,0,0`
	`Physical Address=NeuronID 000239712501`
	`(00256)vxWorks Image (00001) 00257 v2.00.77`
	`(PID=0:OID=1) Serial=N/A`
	`(00256)BootROM (00001) 00258 v2.00.76`
	`(PID=0:OID=2) Serial=N/A`
	`(00256)AXLink I/F uContr(00001) 00270 v1.02`
	`(PID=0:OID=3) Serial=0000000000000000`
	`00096 (00192)VOLUME 3 CONTROL BO(00001)AMX Corp. 00000 v2.10`
	`(PID=0:OID=0) Serial=0000000000000000`
	`Physical Address=Axlink`
	`00128 (00188)COLOR LCD TOUCH PAN(00001)AMX Corp. 32778 v5.01d`
	`(PID=0:OID=0) Serial=0000000000000000`
	`Physical Address=Axlink`
	`05001 (00257)NXI Download (00001)AMX Corp. 00260 v1.00.20`
	`(PID=0:OID=0) Serial=0,0,0,0,0,0,0,0,0,0,0,0,`
	`Physical Address=NeuronID 000189145801`
	`(00257)NXI/NXI-1000 Boot(00001) 00261 v1.00.00`
	`(PID=0:OID=1) Serial=0,0,0,0,0,0,0,0,0,0,0,0,`
	`10002 (00003)PHAST PLK-IMS (00001)Phast Corp. 0003 v3.12`
	`(PID=0:OID=0) Serial=0000000000000000`
	`Physical Address=NeuronID 0100417BD800`

Program Port Commands (Cont.)	
Command	**Description**

TCP LIST	Lists all active TCP/IP connections.
	Example:
	`>TCP LIST`
	`The following TCP connections exist(ed):`
	`1: IP=192.168.21.56:1042 Socket=0 (Dead)`
	`2: IP=192.168.21.56:1420 Socket=0 (Dead)`

URL LIST <D:P:S>	Displays the list of URL addresses programmed in the Master Card (or another system).
	Example:
	`>URL LIST`
	`The following URLs exist in the URL connection list`
	`->Entry 0-192.168.13.65:1319 IP=192.168.13.65 State=Connected`
	`Entry 1-192.168.13.200:1319 IP=192.168.13.200 State=Issue Connect`

ESC Pass Codes

There are 'escape' codes in the pass mode. These codes can switch the display mode or exit the pass mode. The following 'escape' codes are defined.

ESC Pass Codes	
Command	**Description**
+ + ESC ESC Exit Pass Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by another escape exits the pass mode. The Telnet session returns to "normal".
+ + ESC A ASCII Display Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'A' sets the display to ASCII mode. Any ASCII characters received by the device will be displayed by their ASCII symbol. Any non-ASCII characters will be displayed with a \ followed by two hex characters to indicate the character's hex value.
+ + ESC D Decimal Display Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'D' sets the display to decimal mode. Any characters received by the device will be displayed with a \ followed by numeric characters to indicate the character's decimal value.
+ + ESC H Hex Display Mode	Typing a plus (shift =) followed by another plus followed by an ESC (the escape key) followed by an 'H' sets the display to hexadecimal mode. Any characters received by the device will be displayed with a \ followed by two hex characters to indicate the character's hex value.

Notes on Specific Telnet/Terminal Clients

Telnet and terminal clients will have different behaviors in some situations. This section states some of the known anomalies.

Windows client programs

Anomalies occur when using a windows client if you are not typing standard ASCII characters (i.e. using the keypad and the ALT key to enter decimal codes). Most programs will allow you to enter specific decimal codes by holding ALT and using keypad numbers.

For example, hold ALT, hit keypad 1, then hit keypad 0, then release ALT. The standard line feed code is entered (decimal 10). Windows will perform an AnsiToOem conversion on some codes entered this way because of the way Windows handles languages and code pages. The following codes are known to be altered, but others may be affected depending on the computer's setup.

- Characters 15, 21, and 22
- Any characters above 127

This affects both Windows Telnet and Terminal programs.

Linux Telnet client

The Linux Telnet client has three anomalies that are known at this time:

- A null (\00) character is sent after a carriage return.
- If an ALT 255 is entered, two 255 characters are sent (per the telnet RFC).
- If the code to go back to command mode is entered (ALT 29 which is `^]`), the character is not sent, but telnet command mode is entered.

AMX reserves the right to alter specifications without notice at any time.

ARGENTINA • AUSTRALIA • BELGIUM • BRAZIL • CANADA • CHINA • ENGLAND • FRANCE • GERMANY • GREECE • HONG KONG • INDIA • INDONESIA • ITALY • JAPAN
LEBANON • MALAYSIA • MEXICO • NETHERLANDS • NEW ZEALAND • PHILIPPINES • PORTUGAL • RUSSIA • SINGAPORE • SPAIN • SWITZERLAND • THAILAND • TURKEY • USA
ATLANTA • BOSTON • CHICAGO • CLEVELAND • DALLAS • DENVER • INDIANAPOLIS • LOS ANGELES • MINNEAPOLIS • PHILADELPHIA • PHOENIX • PORTLAND • SPOKANE • TAMPA

3000 RESEARCH DRIVE, RICHARDSON, TX 75082 USA • 800.222.0193 • 469.624.8000 • 469-624-7153 fax • 800.932.6993 technical support • www.amx.com

060-004-2564 4/04

Last Revision: 04/05/04